PART III

Administer Cisco ISE 77

Administrator Access to Cisco ISE 77
Administrator Login Browser Support 78
Administrator Lockout Following Failed Login Attempts 78
Specify Proxy Settings in Cisco ISE 79

Setup Cisco ISE Management Access 75

CHAPTER 5

Administrator Login Browser Support 78
Administrator Lockout Following Failed Login Attempts 78
Specify Proxy Settings in Cisco ISE 79
Ports Used by the Admin Portal 79
Enable External RESTful Services APIs 79
External RESTful Services SDK 80
Specify System Time and NTP Server Settings 81
Changing the System Time Zone 82
Configure SMTP Server to Support Notifications 82
Cisco ISE Deployment Upgrade 83
  Different Types of Deployment 83
  Upgrade a Distributed Deployment 83
Cisco ISE Software Patches 87
  Software Patch Installation Guidelines 87
  Install a Software Patch 88
Roll Back Software Patches 88
  Software Patch Rollback Guidelines 89
View Patch Install and Rollback Changes 89
FIPS Mode Support 90
  Enable FIPS Mode in Cisco ISE 91
  Configure Cisco ISE for Administrator CAC Authentication 91
Securing SSH Key Exchange Using Diffie-Hellman Algorithm 94
Configure Cisco ISE to Send Secure Syslog 94
  Configure Secure Syslog Remote Logging Target 95
  Enable Logging Categories to Send Auditable Events to the Secure Syslog Target 95
  Disable the TCP Syslog and UDP Syslog Collectors 96
Default Secure Syslog Collector 96
Offline Maintenance 97

CHAPTER 6

Manage Administrators and Admin Access Policies 99
  Role-Based Access Control 99
  Cisco ISE Administrators 99
    Privileges of a CLI Administrator Versus a Web-Based Administrator 100
    Create a New Cisco ISE Administrator 100
  Cisco ISE Administrator Groups 101
    Create Admin Groups 110
  Administrative Access to Cisco ISE 111
<table>
<thead>
<tr>
<th>Role-Based Access Control in Cisco ISE</th>
<th>111</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role-Based Permissions</td>
<td>111</td>
</tr>
<tr>
<td>RBAC Policies</td>
<td>112</td>
</tr>
<tr>
<td>Default Menu Access Permissions</td>
<td>112</td>
</tr>
<tr>
<td>Configure Menu Access Permissions</td>
<td>112</td>
</tr>
<tr>
<td>Prerequisites for Granting Data Access Permissions</td>
<td>113</td>
</tr>
<tr>
<td>Default Data Access Permissions</td>
<td>113</td>
</tr>
<tr>
<td>Configure Data Access Permissions</td>
<td>115</td>
</tr>
<tr>
<td>The Read-Only Admin Policy</td>
<td>115</td>
</tr>
<tr>
<td>Customize Menu Access for the Read-Only Administrator</td>
<td>115</td>
</tr>
<tr>
<td>Configure Admin Access Policies</td>
<td>116</td>
</tr>
<tr>
<td>Administrator Access Settings</td>
<td>117</td>
</tr>
<tr>
<td>Configure the Maximum Number of Concurrent Administrative Sessions and Login Banners</td>
<td>117</td>
</tr>
<tr>
<td>Allow Administrative Access to Cisco ISE from Select IP Addresses</td>
<td>117</td>
</tr>
<tr>
<td>Configure a Password Policy for Administrator Accounts</td>
<td>118</td>
</tr>
<tr>
<td>Configure Account Disable Policy for Administrator Accounts</td>
<td>119</td>
</tr>
<tr>
<td>Configure Lock or Suspend Settings for Administrator Accounts</td>
<td>119</td>
</tr>
<tr>
<td>Configure Session Timeout for Administrators</td>
<td>120</td>
</tr>
<tr>
<td>Terminate an Active Administrative Session</td>
<td>120</td>
</tr>
<tr>
<td>Change Administrator Name</td>
<td>120</td>
</tr>
<tr>
<td>Administrative Access to Cisco ISE Using an External Identity Store</td>
<td>121</td>
</tr>
<tr>
<td>External Authentication and Authorization</td>
<td>121</td>
</tr>
<tr>
<td>External Authentication Process Flow</td>
<td>122</td>
</tr>
<tr>
<td>Configure a Password-Based Authentication Using an External Identity Store</td>
<td>122</td>
</tr>
<tr>
<td>Create an External Administrator Group</td>
<td>122</td>
</tr>
<tr>
<td>Create an Internal Read-Only Admin</td>
<td>123</td>
</tr>
<tr>
<td>Map External Groups to the Read-Only Admin Group</td>
<td>123</td>
</tr>
<tr>
<td>Configure Menu Access and Data Access Permissions for the External Administrator Group</td>
<td>123</td>
</tr>
<tr>
<td>Create an RBAC Policy for External Administrator Authentication</td>
<td>124</td>
</tr>
<tr>
<td>Configure Admin Access Using an External Identity Store for Authentication with Internal Authorization</td>
<td>124</td>
</tr>
</tbody>
</table>

**CHAPTER 7**

<table>
<thead>
<tr>
<th>Cisco ISE Licenses</th>
<th>127</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ISE Licenses</td>
<td>127</td>
</tr>
</tbody>
</table>
Manage Traditional License Files 128
Cisco ISE Licensing Model 128
Traditional License Consumption 131
View License Consumption 132
Unregistered License Consumption 133
Manage License Files 133
Register Licenses 133
Re-Host Licenses 134
Renew Licenses 134
Migrate and Upgrade Licenses 134
Remove Licenses 135

CHAPTER 8

Manage Certificates 137
Certificate Management in Cisco ISE 137
  Certificates Enable Cisco ISE to Provide Secure Access 137
Certificate Usage 138
Certificate Matching in Cisco ISE 139
Validity of X.509 Certificates 140
Enable PKI in Cisco ISE 140
Wildcard Certificates 141
  Wildcard Certificate Support in Cisco ISE 142
  Wildcard Certificates for HTTPS and EAP Communication 142
  Fully Qualified Domain Name in URL Redirection 143
  Advantages of Using Wildcard Certificates 144
  Disadvantages of Using Wildcard Certificates 144
  Wildcard Certificate Compatibility 145
Certificate Hierarchy 145
System Certificates 145
  View System Certificates 146
  Import a System Certificate 147
  Generate a Self-Signed Certificate 148
  Edit a System Certificate 149
  Delete System Certificate 149
  Export a System Certificate 150
Contents

- Edit a Cisco ISE CA Certificate 168
- Export a Cisco ISE CA Certificate 168
- Import a Cisco ISE CA Certificate 169

Certificate Templates 169
- Certificate Template Name Extension 169
- Use Certificate Template Name in Authorization Policy Conditions 170
- Deploy Cisco ISE CA Certificates for pxGrid Controller 170

Simple Certificate Enrollment Protocol Profiles 171

Issued Certificates 171
- Backup and Restore of Cisco ISE CA Certificates and Keys 172
  - Export Cisco ISE CA Certificates and Keys 172
  - Import Cisco ISE CA Certificates and Keys 173
- Generate Root CA and Subordinate CAs on the Primary PAN and PSN 174
- Configure Cisco ISE Root CA as Subordinate CA of an External PKI 174

Configure Cisco ISE to Use Certificates for Authenticating Personal Devices 175
- Add Users to the Employee User Group 175
- Create a Certificate Authentication Profile for TLS-Based Authentication 176
- Create an Identity Source Sequence for TLS-Based Authentication 176
- Configure Certificate Authority Settings 177
- Create a CA Template 178
- Create a Native Supplicant Profile to be Used in Client Provisioning Policy 179
- Download Agent Resources from Cisco Site for Windows and MAC OS X Operating Systems 180
- Create Client Provisioning Policy Rules for Apple iOS, Android, and MACOSX Devices 180
- Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication 181
- Create Authorization Profiles for Central Web Authentication and Supplicant Provisioning Flows 182
- Create Authorization Policy Rules 182

CA Service Policy Reference 183
- Client Provisioning Policy Rules for Certificate Services 183
- Authorization Profiles for Certificate Services 184
- Authorization Policy Rules for Certificate Services 185

ISE CA Issues Certificates to ASA VPN Users 186
- VPN Connection Certificate Provisioning Flow 186
Required Permissions when AD User not in Domain Admin Group 248
Permissions to Use DCOM on the Domain Controller 249
Set Permissions for Access to WMI Root/CIMv2 Name Space 251
Set Permissions When AD User in the Domain Admin Group 252
Required Permissions when AD User not in Domain Admin Group 253
Permissions to Use DCOM on the Domain Controller 254
Set Permissions for Access to WMI Root/CIMv2 Name Space 255
Open Firewall Ports for WMI Access 256
Configure an Authorization Profile for Redirecting Nonregistered Devices 257
Configure Authorization Policy Rules for the MDM Use Cases 257
Wipe or Lock a Device 258
View Mobile Device Manager Reports 258
View Mobile Device Manager Logs 259

CHAPTER 11 Manage Resources 261
Dictionaries and Dictionary Attributes 261
System Defined Dictionaries and Dictionary Attributes 261
Display System Dictionaries and Dictionary Attributes 262
User-Defined Dictionaries and Dictionary Attributes 262
Create User-Defined Dictionaries 262
Create User-Defined Dictionary Attributes 263
RADIUS-Vendor Dictionaries 263
Create RADIUS-Vendor Dictionaries 264
Create RADIUS-Vendor Dictionary Attributes 264
HP RADIUS IETF Service Type Attributes 264

CHAPTER 12 Logging Mechanism 267
Cisco ISE Logging Mechanism 267
Configure Local Log Purge Settings 267
Cisco ISE System Logs 268
Local Store Syslog Message Format 268
Remote Syslog Message Format 270
Configure Remote Syslog Collection Locations 272
Cisco ISE Message Codes 273
Set Severity Levels for Message Codes 273
Cisco ISE Message Catalogs 274
Debug Logs 274
  View Logging Components for a Node 274
  Configure Debug Log Severity Level 274
Endpoint Debug Log Collector 275
  Download Debug Logs for a Specific Endpoint 275
Collection Filters 276
  Configure Collection Filters 276
  Event Suppression Bypass Filter 276

CHAPTER 13 Backup and Restore Operations 279
Backup Data Type 279
Backup and Restore Repositories 280
  Create Repositories 280
  Enable RSA Public Key Authentication in SFTP Repository 282
On-Demand and Scheduled Backups 282
  Perform an On-Demand Backup 283
  Schedule a Backup 284
Backup Using the CLI 286
Backup History 286
Backup Failures 286
Cisco ISE Restore Operation 287
  Guidelines for Data Restoration 287
  Restoration of Configuration or Monitoring (Operational) Backup from the CLI 288
  Restore Configuration Backups from the GUI 290
  Restoration of Monitoring Database 291
    Restore a Monitoring (Operational) Backup in a Standalone Environment 291
    Restore a Monitoring Backup with Administration and Monitor Personas 292
    Restore a Monitoring Backup with a Monitoring Persona 293
  Restore History 293
  Export Authentication and Authorization Policy Configuration 293
  Synchronize Primary and Secondary Nodes in a Distributed Environment 294
  Recovery of Lost Nodes in Standalone and Distributed Deployments 294
Recovery of Lost Nodes Using Existing IP Addresses and Hostnames in a Distributed Deployment 295
Recovery of Lost Nodes Using New IP Addresses and Hostnames in a Distributed Deployment 295
Recovery of a Node Using Existing IP Address and Hostname in a Standalone Deployment 296
Recovery of a Node Using New IP Address and Hostname in a Standalone Deployment 296
Configuration Rollback 297
Recovery of Primary Node in Case of Failure in a Distributed Deployment 297
Recovery of Secondary Node in Case of Failure in a Distributed Deployment 298

CHAPTER 14  Setup Adaptive Network Control 299
   Enable Adaptive Network Control in Cisco ISE 299
   Configure Network Access Settings 299
      Quarantined Endpoints Do Not Renew Authentication Following Policy Change 300
   Adaptive Network Control 301
      Create Authorization Profiles for Network Access through ANC 302
      ANC Operations Fail when IP Address or MAC Address is not Found 302
      Externally Authenticated Administrators Cannot Perform ANC Operations 302
   ANC Quarantine and Unquarantine Flow 303
   ANC NAS Port Shutdown Flow 303
   Endpoints Purge Settings 304

PART IV  Manage Users and End-User Portals 307

CHAPTER 15  Manage Users and External Identity Sources 309
   Cisco ISE Users 309
      User Identity 309
      User Groups 310
      User Identity Groups 310
      User Role 310
      User Account Custom Attributes and Password Policies 310
   Generate Automatic Password for Users and Administrators 313
   Add Users 313
   Export Cisco ISE User Data 314
   Import Cisco ISE Internal Users 314
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Setup and Configuration</td>
<td>360</td>
</tr>
<tr>
<td>PassiveID Work Center Dashboard</td>
<td>361</td>
</tr>
<tr>
<td>Active Directory as a Probe and a Provider</td>
<td>362</td>
</tr>
<tr>
<td>Getting Started with the PassiveID Setup</td>
<td>362</td>
</tr>
<tr>
<td>Manage the Active Directory Provider</td>
<td>365</td>
</tr>
<tr>
<td>Active Directory Settings</td>
<td>365</td>
</tr>
<tr>
<td>Additional Passive Identity Service Providers</td>
<td>368</td>
</tr>
<tr>
<td>Active Directory Agents</td>
<td>370</td>
</tr>
<tr>
<td>Automatically Install and Deploy Active Directory (AD) Agents</td>
<td>371</td>
</tr>
<tr>
<td>Manually Install and Deploy Active Directory (AD) Agents</td>
<td>372</td>
</tr>
<tr>
<td>Uninstall the Agent</td>
<td>373</td>
</tr>
<tr>
<td>Active Directory (AD) Agent Settings</td>
<td>373</td>
</tr>
<tr>
<td>API Providers</td>
<td>374</td>
</tr>
<tr>
<td>Configure a Bridge to the ISE REST Service for Passive Identity Services</td>
<td>376</td>
</tr>
<tr>
<td>Send API Calls to the Passive ID REST Service</td>
<td>376</td>
</tr>
<tr>
<td>API Provider Settings</td>
<td>377</td>
</tr>
<tr>
<td>API Calls</td>
<td>377</td>
</tr>
<tr>
<td>SPAN</td>
<td>379</td>
</tr>
<tr>
<td>Working with SPAN</td>
<td>379</td>
</tr>
<tr>
<td>SPAN Settings</td>
<td>380</td>
</tr>
<tr>
<td>Syslog Providers</td>
<td>381</td>
</tr>
<tr>
<td>Configure Syslog Clients</td>
<td>382</td>
</tr>
<tr>
<td>Customize Syslog Message Structures (Templates)</td>
<td>386</td>
</tr>
<tr>
<td>Work with Syslog Pre-Defined Message Templates</td>
<td>391</td>
</tr>
<tr>
<td>Filter Passive Identity Services</td>
<td>402</td>
</tr>
<tr>
<td>Endpoint Probe</td>
<td>403</td>
</tr>
<tr>
<td>Work with the Endpoint Probe</td>
<td>404</td>
</tr>
<tr>
<td>Endpoint Probe Settings</td>
<td>404</td>
</tr>
<tr>
<td>Subscribers</td>
<td>405</td>
</tr>
<tr>
<td>Generate pxGrid Certificates for Subscribers</td>
<td>406</td>
</tr>
<tr>
<td>Enable Subscribers</td>
<td>408</td>
</tr>
<tr>
<td>View Subscriber Events from Live Logs</td>
<td>408</td>
</tr>
<tr>
<td>Configure Subscriber Settings</td>
<td>408</td>
</tr>
<tr>
<td>Monitoring and Troubleshooting Service in PassiveID Work Center</td>
<td>409</td>
</tr>
</tbody>
</table>
Contents

LDAP 409
  LDAP Directory Service 409
  Multiple LDAP Instances 409
  LDAP Failover 410
  LDAP Connection Management 410
  LDAP User Authentication 410
  LDAP Group and Attribute Retrieval for Use in Authorization Policies 411
    LDAP Group Membership Information Retrieval 411
    LDAP Attributes Retrieval 412
    LDAP Certificate Retrieval 412
  Errors Returned by the LDAP Server 412
  LDAP User Lookup 413
  LDAP MAC Address Lookup 413
  Add LDAP Identity Sources 414
    Configure LDAP Schema 414
    Configure Primary and Secondary LDAP Servers 415
    Enable Cisco ISE to Obtain Attributes from the LDAP Server 415
    Retrieve Group Membership Details from the LDAP Server 415
    Retrieve User Attributes From the LDAP Server 416
    Enable Secure Authentication with LDAP Identity Source 416
  ODBC Identity Source 417
    Credential Check for ODBC Database 417
    Add ODBC Identity Source 422
  RADIUS Token Identity Sources 423
    RADIUS Token Server Supported Authentication Protocols 423
    Ports Used By the RADIUS Token Servers for Communication 424
    RADIUS Shared Secret 424
    Failover in RADIUS Token Servers 424
    Configurable Password Prompt in RADIUS Token Servers 424
    RADIUS Token Server User Authentication 424
    User Attribute Cache in RADIUS Token Servers 424
    RADIUS Identity Source in Identity Sequence 425
    RADIUS Server Returns the Same Message for All Errors 425
    Safeword Server Supports Special Username Format 425
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Request and Response in RADIUS Token Servers</td>
<td>426</td>
</tr>
<tr>
<td>Add a RADIUS Token Server</td>
<td>426</td>
</tr>
<tr>
<td>Delete a RADIUS Token Server</td>
<td>427</td>
</tr>
<tr>
<td>RSA Identity Sources</td>
<td>428</td>
</tr>
<tr>
<td>Cisco ISE and RSA SecurID Server Integration</td>
<td>428</td>
</tr>
<tr>
<td>RSA Configuration in Cisco ISE</td>
<td>429</td>
</tr>
<tr>
<td>RSA Agent Authentication Against the RSA SecurID Server</td>
<td>429</td>
</tr>
<tr>
<td>RSA Identity Sources in a Distributed Cisco ISE Environment</td>
<td>429</td>
</tr>
<tr>
<td>RSA Server Updates in a Cisco ISE Deployment</td>
<td>429</td>
</tr>
<tr>
<td>Override Automatic RSA Routing</td>
<td>429</td>
</tr>
<tr>
<td>RSA Node Secret Reset</td>
<td>429</td>
</tr>
<tr>
<td>RSA Automatic Availability Reset</td>
<td>430</td>
</tr>
<tr>
<td>Add RSA Identity Sources</td>
<td>430</td>
</tr>
<tr>
<td>Import the RSA Configuration File</td>
<td>430</td>
</tr>
<tr>
<td>Configure the Options File for a Cisco ISE Server and Resetting SecurID</td>
<td>431</td>
</tr>
<tr>
<td>and sdstatus.12 Files</td>
<td></td>
</tr>
<tr>
<td>Configure Authentication Control Options for RSA Identity Source</td>
<td>432</td>
</tr>
<tr>
<td>Configure RSA Prompts</td>
<td>432</td>
</tr>
<tr>
<td>Configure RSA Messages</td>
<td>433</td>
</tr>
<tr>
<td>SAMLv2 Identity Provider as an External Identity Source</td>
<td>433</td>
</tr>
<tr>
<td>Add a SAML Identity Provider</td>
<td>434</td>
</tr>
<tr>
<td>Delete an Identity Provider</td>
<td>437</td>
</tr>
<tr>
<td>Authentication Failure Log</td>
<td>437</td>
</tr>
<tr>
<td>Identity Source Sequences</td>
<td>438</td>
</tr>
<tr>
<td>Create Identity Source Sequences</td>
<td>439</td>
</tr>
<tr>
<td>Delete Identity Source Sequences</td>
<td>439</td>
</tr>
<tr>
<td>Identity Source Details in Reports</td>
<td>440</td>
</tr>
<tr>
<td>Authentications Dashlet</td>
<td>440</td>
</tr>
<tr>
<td>Identity Source Reports</td>
<td>441</td>
</tr>
<tr>
<td><strong>CHAPTER 16</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Configure Guest Access</strong></td>
<td>443</td>
</tr>
<tr>
<td>Cisco ISE Guest Services</td>
<td>443</td>
</tr>
<tr>
<td>End-User Guest and Sponsor Portals in Distributed Environment</td>
<td>443</td>
</tr>
<tr>
<td>Guest and Sponsor Accounts</td>
<td>444</td>
</tr>
</tbody>
</table>
Guest Types and User Identity Groups 444
Create or Edit a Guest Type 445
Disable a Guest Type 447
Changing Guest Account Attributes 448
Configure Maximum Simultaneous Logins for Endpoint Users 448
Schedule When to Purge Expired Guest Accounts 449
Add Custom Fields for Guest Account Creation 450
Specify Email Addresses and SMTP Servers for Email Notifications 450
Assign Guest Locations and SSIDs 451
Rules for Guest Password Policies 452
Set the Guest Password Policy and Expiration 453
Rules for Guest Username Policies 454
Set the Guest Username Policy 454
SMS Providers and Services 455
  Configure SMS Gateways to Send SMS Notifications to Guests 455
Social Login for Self-Registered Guests 456
  Configuring Social Login 458
Guest Portals 460
  Credentials for Guest Portals 460
Guest Access with Hotspot Guest Portals 461
Guest Access with Credentialed Guest Portals 461
Employee Access with Credentialed Guest Portals 462
Guest Device Compliance 462
Guest Portals Configuration Tasks 462
  Enable Policy Services 463
  Add Certificates for Guest Portals 463
Create External Identity Sources 464
Create Identity Source Sequences 465
Create Endpoint Identity Groups 465
Create a Hotspot Guest Portal 466
Create a Sponsored-Guest Portal 467
Create a Self-Registered Guest Portal 468
Authorize Portals 472
Customize Guest Portals 473
Configure Periodic AUP Acceptance 473
Forcing Periodic AUP 474
Guest Remember Me 474
Sponsor Portals 474
Managing Guest Accounts on the Sponsor Portal 475
Managing Sponsor Accounts 476
Configure Account Content for Sponsor Account Creation 480
Configure a Sponsor Portal Flow 481
Enable Policy Services 481
Add Certificates for Guest Services 481
Create External Identity Sources 482
Create Identity Source Sequences 482
Create a Sponsor Portal 483
Customize Sponsor Portals 484
Configuring Account Content for Sponsor Account Creation 484
Configuring the Time Settings Available to Sponsors 484
Sponsors Cannot Log In to the Sponsor Portal 485
Monitor Guest and Sponsor Activity 486
Metrics Dashboard 486
AUP Acceptance Status Report 487
Guest Accounting Report 487
Master Guest Report 487
Sponsor Login and Audit Report 487
Audit Logging for Guest and Sponsor Portals 488
Guest Access Web Authentication Options 488
NAD with Central WebAuth Process 489
Wireless LAN Controller with Local WebAuth Process 490
Wired NAD with Local WebAuth Process 491
IP Address and Port Values Required for the Login.html Page 491
HTTPS Server Enabled on the NAD 492
Support for Customized Authentication Proxy Web Pages on the NAD 492
Configure Web Authentication on the NAD 492
Device Registration WebAuth Process 493
CHAPTER 17  Support Device Access 495

Personal Devices on a Corporate Network (BYOD) 495
   End-User Device Portals in a Distributed Environment 495
   Global Settings for Device Portals 496

Personal Device Portals 496
   Access Device Portals 497
   Blacklist Portal 497
   Certificate Provisioning Portal 497
   Bring Your Own Device Portal 498
   Client Provisioning Portal 498
   Mobile Device Management Portal 498
   My Devices Portal 499

BYOD Deployment Options and Status Flow 499
   Limit the Number of Personal Devices Registered by Employees 502

Support Device Registration Using Native Supplicants 502
   Operating Systems Supported by Native Supplicants 502
   Allow Employees to Register Personal Devices Using Credentialed Guest Portals 502
   Provide a URL to Reconnect with BYOD Registration 503

Device Portals Configuration Tasks 503
   Enable Policy Services 504
   Add Certificates 505
   Create External Identity Sources 505
   Create Identity Source Sequences 506
   Create Endpoint Identity Groups 506
   Edit the Blacklist Portal 507
   Create a BYOD Portal 509
   Create a Certificate Provisioning Portal 510
   Create a Client Provisioning Portal 511
   Create an MDM Portal 512
   Create a My Devices Portal 514

Create Authorization Profiles 515
   Create Authorization Profiles 515
   Create Authorization Policy Rules 515
Customize Device Portals 516
Manage Personal Devices Added by Employees 516
Display Devices Added by an Employee 516
Errors When Adding Devices to My Devices Portal 517
Devices Deleted from My Devices Portal Remain in Endpoints Database 517
Limit the Number of Personal Devices Registered by Employees 517
Monitor My Devices Portals and Endpoints Activity 517
My Devices Login and Audit Report 518
Registered Endpoints Report 518

CHAPTER 18

Customize End-User Web Portals 519
End-User Portals 519
Customization of End-User Web Portals 519
Portal Content Types 522
Basic Customization of Portals 523
Modify the Portal Theme Colors 523
Change the Portal Display Language 524
Change the Portal Icons, Images, and Logos 525
Update the Portal Banner and Footer Elements 525
Change the Titles, Instructions, Buttons, and Label Text 526
Format and Style Text Box Content 526
Variables for Portal Pages Customization 527
View Your Customization 530
Custom Portal Files 530
Advanced Customization of Portals 531
Configure Portal Customization 531
Portal Theme and Structure CSS Files 531
About Changing Theme Colors with jQuery Mobile 532
Change Theme Colors with jQuery Mobile 534
Location Based Customization 535
User Device Type Based Customization 535
Export a Portal’s Default Theme CSS File 536
Create a Custom Portal Theme CSS File 536
Embed Links in Portal Content 537
PART V

CHAPTER 19

Set Up Policy Conditions 557

Policy Conditions 557

Simple and Compound Conditions 557

Policy Evaluation 558

Create Simple Conditions 558

Create Compound Conditions 559

Profiler Conditions 560

Create a Profiler Condition 560

Posture Conditions 561

Simple Posture Conditions 561

Create Simple Posture Conditions 562
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compound Posture Conditions</td>
<td>562</td>
</tr>
<tr>
<td>Predefined Condition for Enabling Automatic Updates in Windows Clients</td>
<td>562</td>
</tr>
<tr>
<td>Preconfigured Antivirus and Antispyware Conditions</td>
<td>562</td>
</tr>
<tr>
<td>Antivirus and Antispyware Support Chart</td>
<td>563</td>
</tr>
<tr>
<td>Compliance Module</td>
<td>563</td>
</tr>
<tr>
<td>Create Compound Posture Conditions</td>
<td>564</td>
</tr>
<tr>
<td>Create Patch Management Conditions</td>
<td>565</td>
</tr>
<tr>
<td>Create Disk Encryption Conditions</td>
<td>565</td>
</tr>
<tr>
<td>Network Conditions</td>
<td>566</td>
</tr>
<tr>
<td>Configure Endstation Network Conditions</td>
<td>567</td>
</tr>
<tr>
<td>Configure Device Network Conditions</td>
<td>567</td>
</tr>
<tr>
<td>Configure Device Port Network Condition</td>
<td>568</td>
</tr>
<tr>
<td>Create Time and Date Conditions</td>
<td>568</td>
</tr>
</tbody>
</table>

### CHAPTER 20

**Manage Authentication Policies** 569

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco ISE Authentication Policies</td>
<td>569</td>
</tr>
<tr>
<td>Policy Condition Evaluation</td>
<td>570</td>
</tr>
<tr>
<td>Supported Network Access Policy Set Protocols</td>
<td>570</td>
</tr>
<tr>
<td>Supported Authentication Types and Database</td>
<td>570</td>
</tr>
<tr>
<td>Authentication Failures—Policy Result Options</td>
<td>571</td>
</tr>
<tr>
<td>Authentication Policy Terminology</td>
<td>572</td>
</tr>
<tr>
<td>Simple Authentication Policies</td>
<td>572</td>
</tr>
<tr>
<td>Simple Authentication Policy Flow</td>
<td>573</td>
</tr>
<tr>
<td>Guidelines for Configuring Simple Authentication Policies</td>
<td>574</td>
</tr>
<tr>
<td>Rule-Based Authentication Policies</td>
<td>574</td>
</tr>
<tr>
<td>Rule-Based Authentication Policy Flow</td>
<td>574</td>
</tr>
<tr>
<td>Supported Dictionaries for Rule-Based Authentication Policies</td>
<td>575</td>
</tr>
<tr>
<td>Attributes Supported by Dictionaries</td>
<td>576</td>
</tr>
<tr>
<td>Policy Set Protocol Settings</td>
<td>579</td>
</tr>
<tr>
<td>Guidelines for Using EAP-FAST as Protocol</td>
<td>579</td>
</tr>
<tr>
<td>Configure EAP-FAST Settings</td>
<td>580</td>
</tr>
<tr>
<td>Generate the PAC for EAP-FAST</td>
<td>580</td>
</tr>
<tr>
<td>Using EAP-TTLS as Authentication Protocol</td>
<td>580</td>
</tr>
<tr>
<td>Configure EAP-TTLS Settings</td>
<td>581</td>
</tr>
</tbody>
</table>
Contents

Configure EAP-TLS Settings 581
Configure PEAP Settings 582
Configure RADIUS Settings 582
Configure Security Settings 582

Network Access Service 584
Define Allowed Protocols for Network Access 584
Enable MAB from Non-Cisco Devices 585
Enable MAB from Cisco Devices 587

Network Access Work Center 588
Cisco ISE Acting as a RADIUS Proxy Server 588
Configure External RADIUS Servers 589
Define RADIUS Server Sequences 589

Cisco ISE Acting as a TACACS+ Proxy Client 590
TACACS+ External Server Settings 590
Configure External TACACS+ Servers 591
TACACS+ Server Sequence Settings 592
Define TACACS+ Server Sequences 593

Location Based Authorization 593
Add a MSE server 594
Location Tree 595

Policy Modes 595
Change Policy Modes 596

Configure a Simple Authentication Policy 596
Configure a Rule-Based Authentication Policy 597
Default Authentication Policy 598

Policy Sets 598
Policy Set Evaluation Flow 599

Configure Policy Sets 600
Global Authorization Exception Policy 600
Configure Policy Sets 601

Authentication Policy Built-In Configurations 601

View Authentication Results 604
Authentication Dashlet 604
Authentication Reports and Troubleshooting Tools 605
CHAPTER 21

Manage Authorization Policies and Profiles 607
Cisco ISE Authorization Policies 607
Cisco ISE Authorization Profiles 607
Authorization Policy Terminology 608
Network Authorization 608
Policy Elements 608
Authorization Profile 608
Authorization Policy 609
Access Control Lists 609
Authorization Policies and Supported Dictionaries 610
Guidelines for Configuring Authorization Policies and Profiles 610
Default Authorization Policies 611
Configure Authorization Policies 612
Authorization Policy Attributes and Conditions 613
Time and Date Conditions 614
Use IPv6 Condition Attributes in Authorization Policies 614
Permissions for Authorization Profiles 616
Configure Permissions for New Standard Authorization Profiles 616
Downloadable ACLs 617
Configure Permissions for Downloadable ACLs 617
Machine Access Restriction for Active Directory User Authorization 618

CHAPTER 22

Configure Threat Centric NAC Service 619
Threat Centric NAC Service 619
Enable Threat Centric NAC Service 622
Add SourceFire FireAMP Adapter 622
Configure Cognitive Threat Analytics Adapter 623
Configure Authorization Profiles for CTA Adapter 625
Configure Authorization Policy using the Course of Action Attribute 625
Support for Vulnerability Assessment in Cisco ISE 626
Enable and Configure Vulnerability Assessment Service 627
Enable Threat Centric NAC Service 627
Configure Qualys Adapter 628
CHAPTER 23
Configure Smart Licensing and Smart Call Home Services 637
Cisco ISE Smart Licensing 637
Activate and Register Smart Licensing in ISE 638
Manage Smart Licensing in ISE 640
Smart Call Home 641
Smart Call Home Profiles 641
Anonymous Reporting 642
Register for Smart Call Home Service 642

CHAPTER 24
Cisco ISE Endpoint Profiling Policies 643
Cisco ISE Profiling Service 643
Profiler Work Center 644
Profiler Dashboard 644
Endpoint Inventory Using Profiling Service 644
Cisco ISE Profiler Queue Limit Configuration 645
Configure Profiling Service in Cisco ISE Nodes 645
Network Probes Used by Profiling Service 646
IP Address and MAC Address Binding 646
NetFlow Probe 647
DHCP Probe 647
Wireless LAN Controller Configuration in DHCP Bridging Mode 648
DHCP SPAN Probe 648
HTTP Probe 648
HTTP SPAN Probe 648
Unable to Collect HTTP Attributes in Cisco ISE Running on VMware 649
RADIUS Probe 649
Network Scan (NMAP) Probe 649
SNMP Read Only Community Strings for NMAP Manual Subnet Scan 650
Manual NMAP Scan Results 650

DNS Probe 651
    DNS FQDN Lookup 651
    Configure Call Station ID Type in the WLC Web Interface 651

SNMP Query Probe 652
    Cisco Discovery Protocol Support with SNMP Query 652
    Link Layer Discovery Protocol Support with SNMP Query 652

SNMP Trap Probe 653

Active Directory Probe 654

Configure Probes per Cisco ISE Node 654

Setup CoA, SNMP RO Community, and Endpoint Attribute Filter 655
    Global Configuration of Change of Authorization for Authenticated Endpoints 656
    Use Cases for Issuing Change of Authorization 656
    Exemptions for Issuing a Change of Authorization 657
    Change of Authorization Issued for Each Type of CoA Configuration 658

Attribute Filters for ISE Database Persistence and Performance 658
    Global Setting to Filter Endpoint Attributes with Whitelist 659

Attributes Collection from IOS Sensor Embedded Switches 660
    IOS Sensor Embedded Network Access Devices 661
    Configuration Checklist for IOS Sensor-Enabled Network Access Devices 661

Profiler Conditions 662

Profiling Network Scan Actions 663
    Create a New Network Scan Action 663
        NMAP Operating System Scan 664
        Operating System Ports 664
        NMAP SNMP Port Scan 668
        NMAP Common Ports Scan 668
        Common Ports 669
        NMAP Custom Ports Scan 669
        NMAP Include Service Version Information Scan 670
        NMAP SMB Discovery Scan 670
        Skip NMAP Host Discovery 670
        NMAP Scan Workflow 671
        Exclude Subnets from NMAP Scan 675
<table>
<thead>
<tr>
<th>Contents</th>
</tr>
</thead>
</table>

**CHAPTER 25 Configure Client Provisioning**

- **Configure Client Provisioning in Cisco ISE**
- **Client Provisioning Resources**
- **Add Client Provisioning Resources from Cisco**
- **Add Cisco Provided Client Provisioning Resources from a Local Machine**
- **Add Customer Created Resources for AnyConnect from a Local Machine**
- **Create Native Supplicant Profiles**
  - **Native Supplicant Profile Settings**
- **Client Provisioning Without URL Redirection for Different Networks**
- **AMP Enabler Profile Settings**
  - **Create an AMP Enabler Profile Using the Embedded Profile Editor**
  - **Create an AMP Enabler Profile Using the Standalone Editor**
  - **Troubleshoot Common AMP Enabler Installation Errors**
- **Cisco ISE Support for Onboarding Chromebook Devices**
  - **Best Practices for Using Chromebook Device in a Shared Environment**
  - **Chromebook Onboarding Process**
  - **Configure the Network and Force Extensions in the Google Admin Console**
  - **Configure ISE for Chromebook Onboarding**
  - **Wipe a Chromebook Device**
  - **Enroll Chromebook to the Google Admin Console**
  - **Connect Chromebook to the Cisco ISE Network for BYOD Onboarding**
  - **Google Admin Console - Wi-Fi Network Settings**
  - **Monitor Chromebook Device Activities in Cisco ISE**
  - **Troubleshoot Chromebook Device Onboarding**
- **Create AnyConnect Configuration**
Create a Posture Agent Profile 760
Client IP Address Refresh Configuration 760
Posture Protocol Settings 763
Client Login Session Criteria 763
Agent Download Issues on Client Machine 764
Cisco ISE Posture Agents 764
Posture Agent Discovery Request and Cisco ISE Response 764
Web Agent Posture Discovery Request and Cisco ISE Response 765
Agent Displays “Temporary Access” 765
Agent Fails to Initiate Posture Assessment 766
AnyConnect 766
Cisco Web Agent 767
Configure Client Provisioning Resource Policies 767
Configure Cisco ISE Posture Agent in the Client Provisioning Policy 768
Configure Native Supplicants for Personal Devices 769
Client Provisioning Reports 769
Client Provisioning Event Logs 770

CHAPTER 26 Configure Client Posture Policies 771
Posture Service 772
Components of Posture Services 772
Posture and Client-Provisioning Policies Workflow 774
Posture Service Licenses 774
Posture Service Deployment 774
Enable Posture Session Service in Cisco ISE 775
Run the Posture Assessment Report 775
Posture Administration Settings 775
Timer Settings for Clients 776
Set Remediation Timer for Clients to Remediate Within Specified Time 776
Set Network Transition Delay Timer for Clients to Transition 776
Set Login Success Window to Close Automatically 777
Set Posture Status for Nonagent Devices 777
Posture Lease 778
Periodic Reassessments 778
Configure Periodic Reassessments 778
Download Posture Updates to Cisco ISE 779
  Download Posture Updates Automatically 780
Configure Acceptable Use Policies for Posture Assessment 780
Posture Conditions 780
Simple Posture Conditions 781
Create Simple Posture Conditions 781
Compound Posture Conditions 782
Predefined Condition for Enabling Automatic Updates in Windows Clients 782
Preconfigured Antivirus and Antispyware Conditions 782
Antivirus and Antispyware Support Chart 783
Compliance Module 783
Create Compound Posture Conditions 784
Create Patch Management Conditions 785
Create Disk Encryption Conditions 785
Configure Posture Policies 786
Prerequisite for Certificate-Based Conditions 787
Default Posture Policies 788
Posture Assessment Options 789
Posture Remediation Options 790
Custom Conditions for Posture 791
Posture End-Point Custom Attributes 791
Create Posture Policy Using End-Point Custom Attributes 791
Custom Posture Remediation Actions 792
  Add a File Remediation 793
  Add a Link Remediation 793
  Add a Patch Management Remediation 793
  Add an Antivirus Remediation 794
  Add an Antispyware Remediation 794
  Add a Launch Program Remediation 795
    Troubleshoot Launch Program Remediation 795
  Add a Windows Update Remediation 795
  Add a Windows Server Update Services Remediation 796
Posture Assessment Requirements 796
Client System Stuck in Noncompliant State 797
Create Client Posture Requirements 797
Custom Permissions for Posture 798
Configure Standard Authorization Policies 799
Best Practices for Network Drive Mapping with Posture 799
AnyConnect Stealth Mode Workflow 799

Create an AnyConnect Agent Profile 800
Create an AnyConnect Configuration for AnyConnect Packages 800
Upload a Open DNS Profile in Cisco ISE 801
Create a Client Provisioning Policy 801
Create a Posture Condition 801
Create Posture Remediation 802
Create Posture Requirement in Stealth Mode 802
Create Posture Policy 802

Posture Types 803

Cisco Temporal Agent Workflow 804

Create Posture Condition 804
Create Posture Requirements 805
Create the Posture Policy 805
Configure the Client Provisioning Policy 805
Download and Launch Cisco Temporal Agent 806

CHAPTER 27
Cisco TrustSec Policies Configuration 807

TrustSec Architecture 807

TrustSec Components 808
TrustSec Terminology 809

Supported Switches and Required Components for TrustSec 810
Integration with Cisco Digital Network Architecture Center (DNA-C) 810

TrustSec Dashboard 811

Metrics 812

Current Network Status 812
Active SGT Sessions 812
Alarms 812
Quick View 813
Live Log 814
Configure TrustSec Global Settings 814
Configure TrustSec Matrix Settings 815
Configure TrustSec Devices 815
OOB TrustSec PAC 815
    Generate a TrustSec PAC from the Settings Screen 816
    Generate a TrustSec PAC from the Network Devices Screen 816
    Generate a TrustSec PAC from the Network Devices List Screen 816
Push Button 817
Configure TrustSec AAA Servers 817
Security Groups Configuration 818
    Add Security Groups 818
    Import Security Groups into Cisco ISE 819
    Export Security Groups from Cisco ISE 819
    Add IP SGT Static Mapping 820
    Import IP SGT Static Mappings into Cisco ISE 820
    Export IP SGT Static Mappings from Cisco ISE 820
    Add SGT Mapping Group 821
    Add Security Group Access Control Lists 821
Egress Policy 823
    Source Tree View 824
    Destination Tree View 824
    Matrix View 824
        Matrix Dimensions 825
        Import/Export Matrix 825
        Create Custom View 825
        Matrix Operations 826
    Configure Work Process Settings 826
    Matrices Listing Page 827
    TrustSec Matrix Workflow Process 828
Egress Policy Table Cells Configuration 833
    Add the Mapping of Egress Policy Cells 833
    Export Egress Policy 834
    Import Egress Policy 834
CPART VI

Monitoring and Troubleshooting Cisco ISE 853

CHAPTER 28

Monitoring and Troubleshooting 855

Monitoring and Troubleshooting Service in Cisco ISE 855
Cisco ISE Dashboard 856
NPF Event Flow Process 858
User Roles and Permissions for Monitoring and Troubleshooting Capabilities 859
Data Stored in Monitoring Database 859
Device Configuration for Monitoring 859
Troubleshooting the Anyconnect Agent Download Issues 859
Troubleshooting the Profiler Feed 859
Posture Compliance 860
Check Posture Compliance 860
SNMP Traps To Monitor Cisco ISE Processes 860
Cisco ISE Alarms 862
Alarm Settings 878
Add Custom Alarms 879
Cisco ISE Alarm Notifications and Thresholds 879
Enable and Configure Alarms 880
Cisco ISE Alarms for Monitoring 880
View Monitoring Alarms 880
Log Collection 880
Alarm Syslog Collection Location 880
Live Authentications 881
Monitor Live Authentications 881
Filter Data in Live Authentications Page 882
Global Search for Endpoints 882
Session Trace for an Endpoint 884
Session Removal from the Directory 886
Authentication Summary Report 886
Troubleshoot Network Access Issues 887
Diagnostic Troubleshooting Tools 887
RADIUS Authentication Troubleshooting Tool 887
Troubleshoot Unexpected RADIUS Authentication Results 887
Execute Network Device Tool 888
Execute IOS Show Commands to Check Configuration 888
Evaluate Configuration Validator Tool 888
Troubleshoot Network Device Configuration Issues 888
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Posture Troubleshooting Tool</td>
<td>889</td>
</tr>
<tr>
<td>Troubleshoot Endpoint Posture Failure</td>
<td>889</td>
</tr>
<tr>
<td>Session Trace Test Cases</td>
<td>889</td>
</tr>
<tr>
<td>Configure Session Trace Test Case</td>
<td>889</td>
</tr>
<tr>
<td>Technical Support Tunnel for Advanced Troubleshooting</td>
<td>890</td>
</tr>
<tr>
<td>Establish a Technical Support Tunnel</td>
<td>891</td>
</tr>
<tr>
<td>TCP Dump Utility to Validate the Incoming Traffic</td>
<td>892</td>
</tr>
<tr>
<td>Use TCP Dump to Monitor Network Traffic</td>
<td>892</td>
</tr>
<tr>
<td>Save a TCP Dump File</td>
<td>893</td>
</tr>
<tr>
<td>Compare Unexpected SGACL for an Endpoint or User</td>
<td>893</td>
</tr>
<tr>
<td>Egress Policy Diagnostic Flow</td>
<td>893</td>
</tr>
<tr>
<td>Troubleshoot Connectivity Issues in a Trustsec-Enabled Network with SXP-IP Mappings</td>
<td>894</td>
</tr>
<tr>
<td>Troubleshoot Connectivity Issues in a Trustsec-Enabled Network with IP-SGT Mappings</td>
<td>894</td>
</tr>
<tr>
<td>Device SGT Tool</td>
<td>895</td>
</tr>
<tr>
<td>Troubleshoot Connectivity Issues in a Trustsec-Enabled Network by Comparing Device SGT Mappings</td>
<td>895</td>
</tr>
<tr>
<td>Download Endpoint Statistical Data From Monitoring Nodes</td>
<td>895</td>
</tr>
<tr>
<td>Obtaining Additional Troubleshooting Information</td>
<td>896</td>
</tr>
<tr>
<td>Cisco ISE Support Bundle</td>
<td>896</td>
</tr>
<tr>
<td>Support Bundle</td>
<td>897</td>
</tr>
<tr>
<td>Download Cisco ISE Log Files</td>
<td>897</td>
</tr>
<tr>
<td>Cisco ISE Debug Logs</td>
<td>898</td>
</tr>
<tr>
<td>Obtain Debug Logs</td>
<td>898</td>
</tr>
<tr>
<td>Cisco ISE Components and the Corresponding Debug Logs</td>
<td>898</td>
</tr>
<tr>
<td>Download Debug Logs</td>
<td>900</td>
</tr>
<tr>
<td>Monitoring Database</td>
<td>901</td>
</tr>
<tr>
<td>Back Up and Restore of the Monitoring Database</td>
<td>901</td>
</tr>
<tr>
<td>Monitoring Database Purge</td>
<td>901</td>
</tr>
<tr>
<td>Guidelines for Purging the Monitoring Database</td>
<td>901</td>
</tr>
<tr>
<td>Operational Data Purging</td>
<td>902</td>
</tr>
<tr>
<td>Purge Older Operational Data</td>
<td>902</td>
</tr>
<tr>
<td>Database Crash/File Corruption Issues</td>
<td>903</td>
</tr>
</tbody>
</table>

**CHAPTER 29**

Reports 905
Cisco ISE Reports 905
Report Filters  905
Create the Quick Filter Criteria  906
Create the Advanced Filter Criteria  906
Run and View Reports  907
Reports Navigation  907
Export Reports  908
Scheduling and Saving the Reports  909
Cisco ISE Active RADIUS Sessions  910
Change Authorization for RADIUS Sessions  910
Available Reports  911

PART VII Reference 913

CHAPTER 30 Administration User Interface Reference 915
Deployment and Node Settings  915
Deployment Settings  915
Deployment Nodes List Page  915
General Node Settings  917
Profiling Node Settings  922
Certificate Store Settings  924
Self-Signed Certificate Settings  924
Certificate-Signing Request Settings  926
Issued and Revoked Certificates  931
Check the Status of the Certificates (OCSP or CRL).  932
System Certificate Import Settings  932
Trusted Certificate Store Page  933
Edit Certificate Settings  934
Trusted Certificate Import Settings  936
OCSP Client Profile Settings  937
Internal CA Settings  939
Certificate Template Settings  940
Logging Settings  941
Remote Logging Target Settings  941
Contents

Logging Category Settings  943
Maintenance Settings  944
  Repository Settings  944
  On-Demand Backup Settings  945
  Scheduled Backup Settings  946
  Schedule Policy Export Settings  947
Admin Access Settings  947
  Administrator Password Policy Settings  947
  Session Timeout and Session Information Settings  949
Settings  950
  Posture General Settings  950
  Posture Reassessment Configuration Settings  951
  Posture Acceptable Use Policy Configuration Settings  953
  EAP-FAST Settings  955
  Generate PAC for EAP-FAST Settings  955
  EAP-TTLS Settings  956
  EAP-TLS Settings  957
  PEAP Settings  958
  RADIUS Settings  958
  General TrustSec Settings  961
  TrustSec Matrix Settings  964
  SMS Gateway Settings  965
  DHCP and DNS Services  967
Identity Management  970
  Endpoints  971
    Endpoint Settings  971
    Endpoint Import from LDAP Settings  973
  Groups  974
    Endpoint Identity Group Settings  974
External Identity Sources  975
  LDAP Identity Source Settings  975
  RADIUS Token Identity Sources Settings  983
  RSA SecurID Identity Source Settings  985
Identity Management Settings  986
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Authentication Policy Settings</td>
<td>986</td>
</tr>
<tr>
<td>Network Resources</td>
<td>988</td>
</tr>
<tr>
<td>Network Devices</td>
<td>988</td>
</tr>
<tr>
<td>Network Device Definition Settings</td>
<td>988</td>
</tr>
<tr>
<td>Default Network Device Definition Settings</td>
<td>998</td>
</tr>
<tr>
<td>Device Security Settings</td>
<td>1000</td>
</tr>
<tr>
<td>Network Device Import Settings</td>
<td>1001</td>
</tr>
<tr>
<td>Network Device Groups</td>
<td>1001</td>
</tr>
<tr>
<td>Network Device Group Settings</td>
<td>1002</td>
</tr>
<tr>
<td>Network Device Group Import Settings</td>
<td>1002</td>
</tr>
<tr>
<td>Network Device Profiles Settings</td>
<td>1003</td>
</tr>
<tr>
<td>External RADIUS Server Settings</td>
<td>1009</td>
</tr>
<tr>
<td>RADIUS Server Sequences</td>
<td>1010</td>
</tr>
<tr>
<td>NAC Manager Settings</td>
<td>1012</td>
</tr>
<tr>
<td>Device Portal Management</td>
<td>1013</td>
</tr>
<tr>
<td>Configure Device Portal Settings</td>
<td>1013</td>
</tr>
<tr>
<td>Global Settings for Device Portals</td>
<td>1013</td>
</tr>
<tr>
<td>Portal Identification Settings for Device Portals</td>
<td>1014</td>
</tr>
<tr>
<td>Portal Settings for the Blacklist Portal</td>
<td>1015</td>
</tr>
<tr>
<td>Portal Settings for BYOD and MDM Portals</td>
<td>1016</td>
</tr>
<tr>
<td>BYOD Settings for BYOD Portals</td>
<td>1018</td>
</tr>
<tr>
<td>Portal Settings for Certificate Provisioning Portal</td>
<td>1020</td>
</tr>
<tr>
<td>Portal Settings for Client Provisioning Portals</td>
<td>1023</td>
</tr>
<tr>
<td>Employee Mobile Device Management Settings for MDM Portals</td>
<td>1025</td>
</tr>
<tr>
<td>Portal Settings for My Devices Portals</td>
<td>1026</td>
</tr>
<tr>
<td>Login Page Settings for My Devices Portals</td>
<td>1028</td>
</tr>
<tr>
<td>Acceptable Use Policy Page Settings for My Devices Portals</td>
<td>1029</td>
</tr>
<tr>
<td>Post-Login Banner Page Settings for My Devices Portals</td>
<td>1029</td>
</tr>
<tr>
<td>Employee Change Password Settings for My Devices Portals</td>
<td>1030</td>
</tr>
<tr>
<td>Manage Device Settings for My Devices Portal</td>
<td>1030</td>
</tr>
<tr>
<td>Add, Edit, and Locate Device Customization for My Devices Portals</td>
<td>1032</td>
</tr>
<tr>
<td>Support Information Page Settings for Device Portals</td>
<td>1032</td>
</tr>
<tr>
<td>Guest Access User Interface Reference</td>
<td>1035</td>
</tr>
</tbody>
</table>
Contents

Guest Portal Settings 1035
  Portal Identification Settings 1035
  Portal Settings for Hotspot Guest Portals 1036
  Acceptable Use Policy (AUP) Page Settings for Hotspot Guest Portals 1038
  Post-Access Banner Page Settings for Hotspot Portals 1038
  Portal Settings for Credentialed Guest Portals 1039
  Login Page Settings for Credentialed Guest Portals 1041
  Self-Registration Page Settings 1042
  Self Registration Success Page Settings 1044
  Acceptable Use Policy (AUP) Page Settings for Credentialed Guest Portals 1045
  Guest Change Password Settings for Credentialed Guest Portals 1046
  Guest Device Registration Settings for Credentialed Guest Portals 1046
  BYOD Settings for Credentialed Guest Portals 1046
  Post-Login Banner Page Settings for Credentialed Guest Portals 1048
  Guest Device Compliance Settings for Credentialed Guest Portals 1048
  VLAN DHCP Release Page Settings for Guest Portals 1048
  Authentication Success Settings for Guest Portals 1049
  Support Information Page Settings for Guest Portals 1049

Sponsor Portal Application Settings 1051
  Portal Identification Settings 1051
  Portal Settings for Sponsor Portals 1052
  Login Settings for Sponsor Portals 1054
  Acceptable Use Policy (AUP) Settings for Sponsor Portals 1055
  Sponsor Change Password Settings for Sponsor Portals 1055
  Post-Login Banner Settings for Sponsor Portals 1055
  Support Information Page Settings for Sponsor Portals 1056
  Notify Guests Customization for Sponsor Portals 1057
  Manage and Approve Customization for Sponsor Portals 1057

Global Settings 1057
  Global Settings for Guest and Sponsor Portals 1057
  Guest Type Settings 1058
  Sponsor Group Settings 1060

CHAPTER 32   Web Portals Customization Reference 1065
Portal Pages Titles, Content and Labels Character Limits 1065
Character Limits for Portal Pages Titles, Content and Labels 1065
Portal Customization 1067
CSS Classes and Descriptions for End-User Portals Page Layout 1067
HTML Support for a Portal Language File 1068
HTML Support for the Blacklist Portal Language File 1068
HTML Support for Bring Your Own Device Portals Language Files 1069
HTML Support for Certificate Provisioning Portal Language Files 1070
HTML Support for Client Provisioning Portals Language Files 1071
HTML Support for Credential Guest Portals Language Files 1072
HTML Support for Hotspot Guest Portals Language Files 1074
HTML Support for Mobile Device Management Portals Language Files 1075
HTML Support for My Devices Portals Language Files 1076
HTML Support for Sponsor Portals Language Files 1077

CHAPTER 33

Policy User Interface Reference 1079
Policy Set Settings 1079
Policy Set Main Page—Configuration Settings 1079
Authentication Policy Configuration Settings 1081
Local and Global Exceptions Configuration Settings 1083
Authorization Policy Settings 1083
Endpoint Profiling Policies Settings 1085
Endpoint Context Visibility Using UDID Attribute 1090
Dictionaries 1090
Special Conditions 1091
Profiler Condition Settings 1092
Posture Condition Settings 1092
File Condition Settings 1092
Firewall Condition Settings 1097
Registry Condition Settings 1097
Application Condition Settings 1099
Continuous Endpoint Attribute Monitoring 1099
Application Condition Settings 1099
Service Condition Settings 1101
Posture Compound Condition Settings  1102
AntiVirus Condition Settings  1103
Antispyware Compound Condition Settings  1105
Antimalware Condition Settings  1106
Dictionary Simple Condition Settings  1108
Dictionary Compound Condition Settings  1109
Patch Management Condition Settings  1110
Disk Encryption Condition Settings  1113
USB Condition Settings  1114
Hardware Attributes Condition Settings  1115
Time and Date Condition Settings  1115

Results  1116
Allowed Protocols  1116
PAC Options  1126
Authorization Profile Settings  1129
Profiling Exception Action Settings  1133
File Remediation  1134
Firewall Remediations  1135
Link Remediation  1136
Application Remediation  1137
Antimalware Remediation  1138
Antivirus Remediation  1139
Antispyware Remediation  1140
Launch Program Remediation  1141
Windows Update Remediation  1142
Windows Server Update Services Remediation  1144
Patch Management Remediation  1146
USB Mass Storage Check Workflow  1148
USB Mass Storage Remediation  1149
Client Posture Requirements  1150

CHAPTER 34

Operations User Interface Reference  1153
RADIUS Live Logs  1153
RADIUS Live Sessions  1156
TACACS Live Logs 1159
Diagnostic Tools 1161
  RADIUS Authentication Troubleshooting Settings 1161
  Execute Network Device Command Settings 1162
  Evaluate Configuration Validator Settings 1163
  Posture Troubleshooting Settings 1164
  TCP Dump Settings 1165
  SXP-IP Mappings 1166
  IP User SGT 1167
  Device SGT Settings 1168
  Progress Details Settings 1169
  Results Summary 1170
Export Summary 1171

CHAPTER 35 1173

Network Access Flows 1173
  Password-Based Authentication 1173
    Secure Authentication Using Encrypted Passwords and Cryptographic Techniques 1173
    Authentication Methods and Authorization Privileges 1174
  RADIUS Protocol Support in Cisco ISE 1174
  Network Access for Users 1174
    RADIUS-Based Protocols Without EAP 1174
    RADIUS-Based Non-EAP Authentication Flow 1175
      Password Authentication Protocol 1175
      RADIUS-Based PAP Authentication in Cisco ISE 1175
      Challenge Handshake Authentication Protocol 1176
      Microsoft Challenge Handshake Authentication Protocol Version 1 1176
      Microsoft Challenge Handshake Authentication Protocol Version 2 1176
  RADIUS-Based EAP Protocols 1176
  RADIUS-Based EAP Authentication Flow 1177
    Extensible Authentication Protocol-Message Digest 5 1178
    Lightweight Extensible Authentication Protocol 1178
    Protected Extensible Authentication Protocol 1178
    Advantages of Using PEAP 1178
    Supported Supplicants for the PEAP Protocol 1178
CHAPTER 36
Switch and Wireless LAN Controller Configuration Required to Support Cisco ISE Functions

Enable Your Switch to Support Standard Web Authentication 1181
Local Username and Password Definition for Synthetic RADIUS Transactions 1182
NTP Server Configuration to Ensure Accurate Log and Accounting Timestamps 1182
Command to Enable AAA Functions 1182
RADIUS Server Configuration on the Switch 1183
Command to Enable RADIUS Change of Authorization (CoA) 1184
Command to Enable Device Tracking and DHCP Snooping 1184
Command to Enable 802.1X Port-Based Authentication 1185
Command to Enable EAP for Critical Authentications 1185
Command to Throttle AAA Requests Using Recovery Delay 1185
VLAN Definitions Based on Enforcement States 1185
Local (Default) ACLs Definition on the Switch 1186
Enable Switch Ports for 802.1X and MAB 1188
Command to Enable EPM Logging 1189
Command to Enable SNMP Traps 1189
Command to Enable SNMP v3 Query for Profiling 1190
Command to Enable MAC Notification Traps for Profiler to Collect 1190
RADIUS Idle-Timeout Configuration on the Switch 1190
Wireless LAN Controller Configuration for iOS Supplicant Provisioning 1191
Configuring ACLs on the Wireless LAN Controller for MDM Interoperability 1191

CHAPTER 37
Supported Management Information Bases for Cisco ISE Endpoint Profiler
IF-MIB 1193
SNMPv2-MIB 1194
IP-MIB 1194
CISCO-CDP-MIB 1194
CISCO-VTP-MIB 1196
CISCO-STACK-MIB 1196
BRIDGE-MIB  1196
OLD-CISCO-INTERFACE-MIB  1196
CISCO-LWAPP-AP-MIB  1197
CISCO-LWAPP-DOT11-CLIENT-MIB  1198
CISCO-AUTH-FRAMEWORK-MIB  1199
EEE8021-PAE-MIB: RFC IEEE 802.1X  1199
HOST-RESOURCES-MIB  1200
LLDP-MIB  1200
THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2017–2018 Cisco Systems, Inc. All rights reserved.
PART I

Introduction

• Cisco ISE Features, on page 1
• Navigate the Admin portal, on page 13
• What Is Wireless Setup, on page 33
Cisco ISE Overview

Cisco ISE is a security policy management platform that provides secure access to network resources. Cisco ISE functions as a policy decision point and enables enterprises to ensure compliance, enhance infrastructure security, and streamline service operations. Cisco ISE allows enterprises to gather real-time contextual
information from networks, users, and devices. The administrator can then use that information to make governance decisions by tying identity to various network elements, including access switches, wireless LAN controllers (WLCs), Virtual Private Network (VPN) gateways, and data center switches. Cisco ISE acts as the policy manager in the Cisco TrustSec solution and supports TrustSec software-defined segmentation.

**ISE Community Resource**

Join the ISE Community to view resources, ask questions, and participate in discussions. See ISE Product Documentation, YouTube Videos, and Training Resources.

**Note** The examples and screenshots provided in the ISE Community resources may be from earlier releases of Cisco ISE. Check the GUI for newer or extra features and updates.

---

**Key Functions**

Cisco ISE is a consolidated policy-based access control system that incorporates a superset of features available in existing Cisco policy platforms. Cisco ISE performs the following functions:

- Combines authentication, authorization, accounting (AAA), posture, and profiler into one appliance

- Provides for comprehensive guest access management for Cisco ISE administrators, sanctioned sponsor administrators, or both

- Enforces endpoint compliance by providing comprehensive client provisioning measures and assessing the device posture for all endpoints that access the network, including 802.1X environments

- Provides support for discovery, profiling, policy-based placement, and monitoring of endpoint devices on the network

- Enables consistent policy in centralized and distributed deployments that allows services to be delivered where they are needed

- Employs advanced enforcement capabilities including TrustSec through the use of Security Group Tags (SGTs) and Security Group Access Control Lists (SGACLs)

- Supports scalability to support a number of deployment scenarios from small office to large enterprise environments

- Facilitates TACACS-enabled device administration through its Work Center. The Work Center menu contains all the device administration pages, which acts as a single start point for ISE administrators. However, pages such as Users, User Identity Groups, Network Devices, Default Network Devices, Network Device Groups, Authentication and Authorization Conditions, are shared with other menu options.

---

**Identity-Based Network Access**

The Cisco ISE solution provides context-aware identity management in the following areas:

- Cisco ISE determines whether users are accessing the network on an authorized, policy-compliant device.

- Cisco ISE establishes user identity, location, and access history, which can be used for compliance and reporting.
- Cisco ISE assigns services based on the assigned user role, group, and associated policy (job role, location, device type, and so on).
- Cisco ISE grants authenticated users with access to specific segments of the network, or specific applications and services, or both, based on authentication results.

**Support for Multiple Deployment Scenarios**

Cisco ISE can be deployed across an enterprise infrastructure, supporting 802.1X wired, wireless, and Virtual Private Networks (VPNs).

The Cisco ISE architecture supports both standalone and distributed (also known as “high-availability” or “redundant”) deployments where one machine assumes the primary role and another “backup” machine assumes the secondary role. Cisco ISE features distinct configurable personas, services, and roles, which allow you to create and apply Cisco ISE services where they are needed in the network. The result is a comprehensive Cisco ISE deployment that operates as a fully functional and integrated system.

Cisco ISE nodes can be deployed with one or more of the Administration, Monitoring, and Policy Service personas—each one performing a different vital part in your overall network policy management topology. Installing Cisco ISE with an Administration persona allows you to configure and manage your network from a centralized portal to promote efficiency and ease of use.

**Support for UCS Hardware**

Cisco ISE 2.3 supports the following hardware platforms:

- SNS-3415 (small)
- SNS-3495 (large)
- SNS-3515 (small)
- SNS-3595 (large)

Refer to Table 3 in the Cisco Identity Services Engine Data Sheet for the hardware specifications.

**Basic User Authentication and Authorization**

User authentication policies in Cisco ISE enable you to provide authentication for a number of user login session types using a variety of standard authentication protocols including, but not limited to, Password Authentication Protocol (PAP), Challenge-Handshake Authentication Protocol (CHAP), Protected Extensible Authentication Protocol (PEAP), and Extensible Authentication Protocol (EAP). Cisco ISE specifies the allowable protocol(s) that are available to the network devices on which the user tries to authenticate and specifies the identity sources from which user authentication is validated.

Cisco ISE allows for a wide range of variables within authorization policies to ensure that only authorized users can access the appropriate resources when they access the network. The initial release of Cisco ISE supports only RADIUS-governed access to the internal network and its resources.
At the most fundamental level, Cisco ISE supports 802.1X, MAC authentication bypass (MAB), and
browser-based Web authentication login for basic user authentication and access via both wired and wireless
networks. Upon receiving an authentication request, the “outer part” of the authentication policy is used to
select the set of protocols that are allowed when processing the request. Then, the “inner part” of the
authentication policy is used to select the identity source that is used to authenticate the request. The identity
source may consist of a specific identity store or an identity store sequence that lists a set of accessible identities
until the user received a definitive authorization response.

Once authentication succeeds, the session flow proceeds to the authorization policy. (There are also options
available that allow Cisco ISE to process the authorization policy even when the authentication did not
succeed.) Cisco ISE enables you to configure behavior for “authentication failed,” “user not found,” and
“process failed” cases, and also to decide whether to reject the request, drop the request (no response is issued),
or continue to the authorization policy. In cases where Cisco ISE continues to perform authorization, you can
use the “AuthenticationStatus” attribute in the “NetworkAccess” dictionary to incorporate the authentication
result as part of the authorization policy.

The authorization policy result is Cisco ISE assigning an authorization profile that might also involve a
downloadable ACL specifying traffic management on the network policy enforcement device. The downloadable
ACL specifies the RADIUS attributes that are returned during authentication and that define the user access
privileges granted once authenticated by Cisco ISE.

---

**Note**

Cisco ISE processes the attributes in the following order while identifying the Authentication session for the
incoming accounting packet:

- For Cisco devices:
  1. Class/State
  2. audit-session-id

- For third party devices:
  1. Class/State
  2. Calling-Station-ID

  3. If the authentication session cannot be identified, Cisco ISE creates a new session ID based on the
     Calling-Station-ID, NAS-Port, and NAS-IP-Address.

---

**Policy Sets**

Network access policies are consolidated together under Policy Sets, which can be accessed from Policy >
Policy Sets. Each policy set is a container defined on the top level of the policy hierarchy, under which all
relevant Authentication and Authorization policy and policy exception rules for that set are configured. Multiple
rules can be defined for both authentication and authorization, all based on conditions. Conditions and additional
related configurations can also be easily accessed and reused directly from the Policy Set interface.
**Support for Common Access Card Functions**

Cisco ISE supports U.S. government users who authenticate themselves using Common Access Card (CAC) authentication devices. A CAC is an identification badge with an electronic chip containing a set of X.509 client certificates that identify a particular employee of, for example, the U.S. Department of Defense (DoD). Access via the CAC requires a card reader into which the user inserts the card and enters a PIN. The certificates from the card are then transferred into the Windows certificate store, where they are available to applications such as the local browser running Cisco ISE.

Benefits of using a CAC card to authenticate include these:

- Common Access Card X.509 certificates are the identity source for 802.1X EAP-TLS authentication.
- Common Access Card X.509 certificates are also the identity source for authentication and authorization to Cisco ISE administration.

Cisco ISE only supports login to the Admin portal. It does not support CAC authentication for the following access methods:

- You cannot use CAC authentication login to manage the Cisco ISE Command Line Interface.
- External REST API (Monitoring and Troubleshooting) and Endpoint Protection Services Adaptive Network Control APIs are outside the scope of the CAC authentication.
- Guest Services and Guest Sponsor Administration access does not support the CAC authentication method in Cisco ISE.

**Client Posture Assessment**

To ensure that the imposed network security measures remain relevant and effective, Cisco ISE enables you to validate and maintain security capabilities on any client machine that accesses the protected network. By employing posture policies that are designed to ensure that the most up-to-date security settings or applications are available on client machines, the Cisco ISE administrator can ensure that any client machine that accesses the network meets, and continues to meet, the defined security standards for enterprise network access. Posture compliance reports provide Cisco ISE with a snapshot of the compliance level of the client machine at the time of user login, as well as any time a periodic reassessment occurs.

Posture assessment and compliance occurs using one of the following agent types available in Cisco ISE:

- Cisco NAC Web Agent—A temporal agent that the users install on their system at the time of login and that is no longer visible on the client machine once the login session terminates.
- Cisco NAC Agent—A persistent agent that, once installed, remains on a Windows or Mac OS X client machine to perform all security compliance functions.
- AnyConnect ISE Agent—A persistent agent that can be installed on Windows or Mac OS X client to perform posture compliance functions.
- Cisco Temporal Agent—A temporary executable file that is run on the client to check the compliance status. The agent is removed from the client machine after the login session is terminated. By default, the agent resides in the Cisco ISE ISO image, and is uploaded to Cisco ISE during installation.
Network Access for Guests

Cisco ISE administrators and employees who are granted appropriate access to the Cisco ISE guest registration portal as guest sponsors can create temporary guest login accounts and specify available network resources to allow guests, visitors, contractors, consultants, and customers to get restricted access to the specified network resources and Internet. Guest access sessions have expiration timers associated with them, so they are effective in controlling guest access to a specific day, time period, and so forth.

All aspects of a guest user session (including account creation and termination) are tracked and recorded in Cisco ISE so that you can provide audit information and troubleshoot session access, as necessary.

Guests can select a social login provider as a way to provide credentials as a self-registered guest, instead of entering username and password in the guest portal. To enable this, you can configure a social media site as an external identity source, and configure a portal that allows users to use that external identity source (social login provider). Facebook is the social login provider supported by this release.

Support for Personal Devices

Cisco ISE allows employees to connect their personal devices, such as laptop computers, mobile phones, tablets, printers, and other network devices on the enterprise network.

Supporting these devices presents difficulties in protecting network services and enterprise data, so you must ensure that both the employees and their devices are authenticated and authorized for network access. With a Plus license, Cisco ISE provides you with the tools you need to allow employees to securely use their personal devices on your corporate network.

Mobile Device Manager Interoperability with Cisco ISE

Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices deployed across mobile operators, service providers, and enterprises. MDM enforces policy on endpoints, but it cannot force users to register their device or force remediation. ISE retrieves policies from the MDM server, and enforces those policies when users register their devices. If the ISE device policy requires MDM, and the device is not compliant with MDM, then ISE redirects the user to the MDM on-boarding portal, and prompts the user to update the device for network access. ISE can also allow internet-only access to users who decline MDM compliance.

Profiled Endpoints on the Network

The Profiler service assists in identifying, locating, and determining the capabilities of all endpoints on your network (known as identities in Cisco ISE), regardless of their device types, to ensure and maintain appropriate access to your enterprise network. The Cisco ISE Profiler function uses a number of probes to collect attributes for all endpoints on your network, and pass them to the Profiler analyzer, where the known endpoints are classified according to their associated policies and identity groups.

The Profiler Feed service allows administrators to retrieve new and updated endpoint profiling policies and the updated OUI database as a feed from a designated Cisco feed server through a subscription in to Cisco ISE.
pxGrid Persona

Cisco pxGrid is used to enable the sharing of contextual-based information from Cisco ISE session directory to other policy network systems such as Cisco Adaptive Security Appliance (ASA). The pxGrid framework can also be used to exchange policy and configuration data between nodes like sharing tags and policy objects between ISE and third party vendors, and for non-ISE related information exchanges such as threat information.

TrustSec Work Center

All TrustSec-related options are consolidated under the TrustSec Work Center menu (Work Centers > TrustSec), so that the administrator can easily access all the TrustSec options at one location.

The TrustSec dashboard is a centralized monitoring tool for the TrustSec network. The Metrics dashlet displays statistics about the behavior of the TrustSec network. The Active SGT Sessions dashlet displays the SGT sessions that are currently active in the network. The Alarms dashlet displays the alarms related to the TrustSec sessions. The Quick View dashlet displays TrustSec-related information for NADs and SGTs.

You can click the TrustSec Sessions link in the Live Log dashlet to view the active TrustSec sessions. You can also view information regarding TrustSec protocol data requests and responses from NADs to Cisco ISE.

TACACS+ Device Administration

Cisco ISE supports device administration using the Terminal Access Controller Access-Control System (TACACS+) security protocol to control and audit the configuration of network devices. The network devices are configured to query ISE for authentication and authorization of device administrator actions, and send accounting messages for ISE to log the actions. It facilitates granular control of who can access which network device and change the associated network settings. An ISE administrator can create policy sets that allow TACACS results, such as command sets and shell profiles, to be selected in authorization policy rules in a device administration access service. The ISE Monitoring node provides enhanced reports related to device administration. The Work Center menu contains all the device administration pages, which acts as a single start point for ISE administrators.

ISE requires a Device Administration license to use TACACS+.

Support for SXP

Source Group Tag (SGT) Exchange Protocol (SXP) is used to propagate the SGTs across network devices that do not have hardware support for TrustSec. SXP is used to transport an endpoint's SGT along with the IP address from one SGT-aware network device to another.

To enable SXP service on a node, check the Enable SXP Service check box in the General SGT Settings page. You must also specify the interface to be used for SXP service.

Each SXP connection has one peer designated as SXP speaker and the other peer as SXP listener. The peers can also be configured in a bi-directional mode where each of them act as both speaker and listener. Connections can be initiated by either peers, but mapping information is always propagated from a speaker to a listener.
Third Party Device Support

Cisco ISE supports some third-party network access devices (NADs) through the use of network device profiles. These profiles define the capabilities that Cisco ISE uses to enable flows such as Guest, BYOD, MAB, and Posture.

Cisco ISE includes predefined profiles for network devices from the following vendors:

- Cisco—Wired and Wireless
- Aruba—Wireless
- HP—Wired and Wireless
- Motorola—Wireless
- Brocade—Wired
- Alcatel—Wired
- Ruckus—Wireless

You can also create profiles for additional third-party network device that does not have a predefined profile. AnyConnect client provisioning and posture discovery do not mandate CoA and URL redirection.

If you have deployed non-Cisco NADs prior to Release 2.0 and created policy rules/RADIUS dictionaries to use them, after upgrade these will continue to work as usual.

Telemetry

After installation, when you log in to the Admin portal for the first time, the Cisco ISE Telemetry banner appears on screen. Using this feature, Cisco ISE securely collects non-sensitive information about your deployment, network access devices, profiler, and other services that you are using. The data that is collected will be used to provide better services and additional features in forthcoming releases. By default, the telemetry feature is enabled. You can choose to disable it from the Admin portal.

IPv6 Support

Cisco ISE, Release 2.0 supports the following IPv6 capabilities:

- Support for IPv6-Enabled Endpoints: Cisco ISE can detect, manage, and secure IPv6 traffic from endpoints. You can configure authorization profiles and policies in Cisco ISE using IPv6 attributes to process requests from IPv6-enabled endpoints and ensure that the endpoint is compliant.
- IPv6 Support in Reports: Reports in Release 2.0 support IPv6 values. The Live Session and Live Authentication pages also support IPv6 values.
  - ipv6 address-To allow for static IPv6 address configuration per network interface
  - ipv6 enable-To enable or disable IPv6 on all network interfaces
  - ipv6 route-To configure IPv6 static routes
Location Based Authorization

Cisco ISE integrates with Cisco Mobility Services Engine (MSE) to introduce physical location-based authorization. Cisco ISE uses information from MSE to provide differentiated network access based on the actual location of the user, as reported by MSE.

With this feature, you can use the endpoint location information to provide network access when a user is in an appropriate zone. You can also add the endpoint location as an additional attribute for policies to define more granulated policy authorization sets based on device location. You can configure conditions within authorization rules that use location-based attributes, for example:

\[ \text{MSE.Location Equals LND_Campus1:Building1:Floor2:SecureZone} \]

You can define the location hierarchy (campus/building/floor structure) and configure the secure and non-secure zones using the Cisco Prime Infrastructure application. After defining the location hierarchy, you must synchronize the location hierarchy data with the MSE servers.

The Location Tree is created by using the location data retrieved from the MSE instances. You can select the location entries that are exposed to the authorization policy by using the Location Tree.

Cisco ISE Certificate Authority

Cisco ISE provides a native Certificate Authority (CA) that issues and manages digital certificates for endpoints from a centralized console to allow employees to connect to the company’s network using their personal devices. Cisco ISE CA supports standalone and subordinate deployments.

Certificate Provisioning Portal

Cisco ISE offers a Certificate Provisioning portal that allows employees to request certificates for devices that cannot go through the onboarding flow. For example, devices such as point-of-sale terminals cannot go through the BYOD flow and need to be issued certificates manually. The Certificate Provisioning portal allows a privileged set of users to upload a certificate request for such devices, generate key pairs (if required), and download the certificate. Employees can access this portal and request for a single certificate or make a bulk certificate request using a CSV file.

Certificate Template Extension

The Cisco ISE Internal CA includes an extension to represent the certificate template that was used to create the endpoint certificate. All endpoint certificates issued by the internal CA contain a certificate template name extension. This extension represents the certificate template that was used to create that endpoint certificate.
You can use the CERTIFICATE: Template Name attribute in authorization policy conditions and assign appropriate access privileges based on the results of the evaluation.

**Cisco ISE Internal CA Issues Certificates to ASA VPN Users**

The internal ISE CA can issue certificates to client machines that connect over ASA VPN. ISE uses the Simple Certificate Enrollment Protocol (SCEP) for enrollment and to provision certificates from Cisco ISE to the client machines.

**Support for Active Directory Multidomain Forests**

Cisco ISE supports Active Directory with multidomain forests. Cisco ISE connects to a single domain, but can access resources from the other domains in the Active Directory forest if trust relationships are established between the domain to which Cisco ISE is connected and the other domains.

**Support for SAnet Devices**

Cisco ISE provides limited support for Session Aware Networking (SAnet), a session management framework on the switches that provides more consistent and flexible management of access-sessions, including visibility, authentication, and authorization. SAnet defines the notion of a service template which is an authorization object accepted both by ISE as well as by the device. This is in contradistinction to Cisco ISE authorization profiles which are containers of RADIUS authorization attributes that are merged and flattened into a list of attributes before they are sent to the device. Similarly, SAnet service templates are also containers of RADIUS authorization attributes but they are not flattened into a list before sending to the device. Instead, Cisco ISE sends the name of the service template and the device downloads the content (RADIUS attributes) if it does not already have a cached or statically defined version of it. In addition, Cisco ISE sends CoA notifications to the device if the definition of a service template has changed, that is, if a RADIUS attribute was added, removed or changed.

Cisco ISE implements service templates as authorization profiles that contain a special flag that marks them as “Service Template” compatible. This way the service template, which is also an authorization profile, can be used in a single policy statement that will support sessions connecting from SAnet capable devices as well as legacy devices.

**Support for Automatic Failover for the Administration Node**

Cisco ISE supports automatic failover for the Administration persona. To enable the auto-failover feature, at least two nodes in your distributed setup should assume the Administration persona and one node should assume the non-Administration persona. If the Primary Administration Node (PAN) goes down, an automatic promotion of the Secondary Administration Node is initiated. For this, a non-administration secondary node is designated as the health check node for each of the administration nodes. The health check node checks the health of PAN at configured intervals. If the health check response received for the PAN health is not good due to being down or not reachable, health check node initiates the promotion of the Secondary Administration Node to take over the primary role after waiting for the configured threshold value. There are some features that are unavailable after auto-failover of the Secondary Administrative Node. Cisco ISE does not support fallback to the original PAN. Refer to the High Availability for the Administrative Node section for more information.
GUI-Based Upgrade

Cisco ISE offers a GUI-based centralized upgrade from the Admin portal. The upgrade process is much simplified and the progress of the upgrade and the status of the nodes are displayed on screen.

Note

The GUI-based upgrade is applicable only if you are upgrading from Release 2.0 to a higher release or if you are upgrading a Limited Availability Release of Cisco ISE 2.0 to the General Availability Release.

Technical Support Tunnel for Advanced Troubleshooting

Cisco ISE uses the Cisco IronPort Tunnel infrastructure to create a secure tunnel for Cisco technical support engineers to connect to an ISE server in your deployment and troubleshoot issues with the system. Cisco ISE uses SSH to create the secure connection through the tunnel. As an administrator, you can control the tunnel access; you can choose when and how long to grant access to the support engineer. Cisco Customer Support cannot establish the tunnel without your intervention. You will receive notification about the service logins. You can disable the tunnel connection at any point of time.
Navigate the Admin portal

- Administrators Portal, on page 13
- Cisco ISE Internationalization and Localization, on page 25
- MAC Address Normalization, on page 31
- Admin Features Limited by Role-Based Access Control Policies, on page 32

Administrators Portal

The Admin portal provides access to ISE configuration and reporting. The following figure shows the main elements of the menu bar of portal.
<table>
<thead>
<tr>
<th></th>
<th>Menu Drop-downs</th>
<th></th>
</tr>
</thead>
</table>
| 1 | • Context Visibility: These menus display information about endpoints, users, and NADs. The information can be segmented by features, applications, BYOD, and other categories, depending on your license. The Context menus use a central database, gathers information from database tables, caches, and buffers, which makes updates to context dashlets and list content very fast. The Context menus consist of dashlets at the top, and a list of information at the bottom. As you filter data by modifying the column attributes in the list, the dashlets are refreshed to show the changed content.
   • Policy: Access tools for managing network security in the areas of authentication, authorization, profiling, posture, and client provisioning.
   • Administration: Access tools for managing Cisco ISE nodes, licenses, certificates, network devices, users, endpoints, and guest services. |
| 2 | Top Right menu |   |
|   | • Search for endpoints and display their distribution by profiles, failures, identity stores, location, device type, and so on. |
|   | • Access online help for the currently displayed page, plus links to the ISE Community, Portal Builder and more. |
|   | • Access the following options: |
|   |   • PassiveID Setup—The **PassiveID Setup** option launches the **PassiveID Setup** wizard to set up passive identity using Active Directory. You can configure the server to gather user identities and IP addresses from external authentication servers and deliver the authenticated IP addresses to the corresponding subscriber. |
|   |   • Visibility Setup—The **Visibility Setup** option launches the **ISE Visibility Setup** wizard that allows you to add a list of IP address range for endpoints discovery. |
|   |   • Wireless Setup (BETA)—The **Wireless Setup (BETA)** option provides an easy way to set up wireless flows for 802.1x, guest, and Bring Your Own Device (BYOD). This option also provides workflows to configure and customize each portal for guest and BYOD. |
|   | • System activities, which includes bringing up the online help, and configuring account settings. |
ISE Home Dashboards

The Cisco ISE Dashboard displays live consolidated and correlated statistical data that is essential for effective monitoring and troubleshooting. Dashboard elements show activity over 24 hours, unless otherwise noted. The following figure shows some of the information available on the Cisco ISE Dashboard. You can view the Cisco ISE Dashboard data only in the Primary Administration Node (PAN).

The Home page has five default dashboards that show a view of your ISE data:

- **Summary**—This view has a linear Metrics dashlet, pie chart dashlets, and list dashlets. The Metrics dashlet is not configurable.
- **Endpoints**—Status, Endpoints, Endpoint Categories, Network Devices.
- **Guests**—Guest user type, logon failures and location.
- **Vulnerability**—Information reported to ISE by vulnerability servers.
- **Threat**—Information reported to ISE by threat servers.

Each of these dashboards has several pre-defined dashlets. For example, the Summary dashboard has: Status, Endpoints, Endpoint Categories, and Network Devices.

### Configuring Home Dashboards

You can customize a Home page dashboard by clicking the gear icon in the upper right-hand corner of the page:
• **Export** saves the currently selected home view to a PDF.

• **Layout Template** configures the number of columns displayed in this view.

• **Manage Dashboards** allows you to make the current dashboard the default (that opens when you select Home), or reset all dashboards (remove your configurations on all the Home dashboards).

## Context Visibility Views

The structure of a Context Visibility page is similar to the Home page, except that Context Visibility pages:

• Retain your current context (browser window) when you filter the displayed data

• Are more customizable

• Focus on endpoint data

You can view the context visibility data only from the Primary Administration Node (PAN).

Dashlets on Context pages show information about endpoints, and endpoint connections to NADs. The information currently displayed is based on the content in the list of data below the dashlets on each page. Each page shows a view of endpoint data, based on the name of the tab. As you filter the data, both the list and dashlets update. You can filter the data by clicking on parts of one or more of the circular graphs, by filtering rows on the table, or any combination those actions. As you select filters, the effects are additive, also referred to as cascading filter, which allows you to drill down to find the particular data you are looking for. You can also click an endpoint in the list, and get a detailed view of that endpoint.

There are four main views under Context Visibility:

• Endpoints—You can select which endpoints to display based on types of devices, compliance status, authentication type, hardware inventory, and more. Refer to the [The Hardware Dashboard, on page 20](#) section for additional information.
We recommend that you enable the accounting settings on the NADs to ensure that the accounting start and update information is sent to Cisco ISE.

Cisco ISE can collect accounting information, such as the latest IP address, status of the session (Connected, Disconnected, or Rejected), inactivity days of an endpoint, only if accounting is enabled. This information is displayed in the Live Logs/Live Sessions and the Context Visibility pages. When accounting is disabled on a NAD, there might be a missing, incorrect, or mismatch in the accounting information between the Live Sessions/ Live Logs and Context Visibility pages.

The Visibility Setup wizard allows you to add a list of IP address range for endpoints discovery. After this wizard is configured, Cisco ISE authenticates the endpoints, but the endpoints that are not included in the configured IP address range are not displayed in the Context Visibility > Endpoints tab and the Endpoints listing page (under Work Centers > Network Access > Identities > Endpoints).

- **User-Based**—Displays user information from user identity sources.
  
  Note the following points while using this view:

  1. If there is any change in the username or password attribute, it will be reflected immediately on this page when there is a change in the authentication status.
  2. If any other attribute other than the username is changed in the Active Directory, the updated attributes are displayed only after 24 hours upon re-authentication.
  3. If the username and other attributes are changed in the Active Directory, the updated changes will be displayed immediately after re-authentication.

- **Network Devices**—List of NADs that have endpoints connected to them. You can click the Number of Endpoints on a NAD (right-most column) to get a Context Visibility screen listing all those devices filtered by that NAD.

  Note

  If you have configured your network device with SNMPv3 parameters, you cannot generate the Network Device Session Status Summary report that is provided by the Monitoring service (Operations > Reports > Catalog > Network Device > Session Status Summary). You can generate this report successfully if your network device is configured with SNMPv1 or SNMPv2c parameters.

- **Application**—The Application view is used to identify the number of endpoints that have a specified application installed. The results are displayed in graphical and table formats. The graphical representation helps you make a comparative analysis. For example, you can find out the number of endpoints with the Google Chrome software along with their Version, Vendor, and Category (Anti-phishing, Browser, and so on) in a table as well as a bar chart. For more information, see The Application Dashboard section.

You can create a new view under Context Visibility to create a custom list, for additional filtering. Dashlets are not supported in custom views for this release.
Clicking a section of a circular graph in a dashlet opens a new page with filtered data from that dashlet in Context Visibility mode. From that new page, you can continue to filter the displayed data, as described in Filtering Displayed Data in a View, on page 22.

For more information about using Context Visibility to find endpoint data, see the following Cisco YouTube video, which uses ISE 2.1 https://www.youtube.com/watch?v=HvonGhrydfg.

Related Topics

The Hardware Dashboard, on page 20

Dashlets

The following picture shows an example dashlet:

1. The stacked window symbol “detaches”, opens this dashlet in a new browser window. The circle refreshes. The X deletes this dashlet, but is only available on the Home page. You delete dashlets in Context Visibility using the gear symbol in the top-right corner of the screen.

2. Some dashlets have different categories of data. Click the link to see a pie chart with that set of data.

3. The Pie chart shows the data that you have selected. Clicking one of the pie segments opens a new tab in Context Visibility with the filtered data, based on that pie segment.

Clicking a section of the pie chart in a Home dashboard opens in new browser window that displays data filtered by the section of the pie chart that you clicked on.

Clicking a section of the pie chart in a Context view filters the displayed data, but does not change the context; the filtered data displays in the same browser window.
The Application Dashboard

Table 1: Description of the Application Dashboard

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The <strong>Summary</strong> tab is selected by default. It displays the <strong>Application Categories</strong> dashlet, which contains a bar chart. Applications are classified into 13 categories. Applications that do not fall into any of these categories are termed Unclassified. The available categories are Anti-Malware, Antiphishing, Backup, Browser, Data Loss Prevention, Data Storage, Encryption, Firewall, Messenger, Patch Management, Public File Sharing, Virtual Machine, and VPN Client.</td>
</tr>
<tr>
<td>2</td>
<td>Each bar corresponds to a classified category. You can hover over each bar to view the total number of applications and endpoints that correspond to the selected application category.</td>
</tr>
<tr>
<td>3</td>
<td>The applications and endpoints that fall under the Classified category are displayed in Blue. Unclassified applications and endpoints are displayed in Gray. You can hover over the classified or unclassified category bar to view the total number of applications and endpoints that belong to that category. You can click <strong>Classified</strong> and view the results in the bar chart and table (5). When you click <strong>Unclassified</strong>, the bar chart is disabled (grayed out) and the results are displayed in the table (5).</td>
</tr>
</tbody>
</table>
The applications and endpoints are displayed based on the selected filter. You can view the breadcrumb trail as you click different filters. You can click **Deselect All** to remove all filters.

![Filter Example](image)

When you click multiple bars, the corresponding classified applications and endpoints are displayed in the table. For example, if you select the Antimalware and Patch Management categories, the following results are displayed.

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Version</th>
<th>Vendor</th>
<th>Category</th>
<th>Application OS</th>
<th>Endpoints With This Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gatekeeper</td>
<td>9.9.5</td>
<td>Apple Inc.</td>
<td>Antimalware</td>
<td>windows 7 64-bit, mac osx 10.10, mac osx 8, mac osx 9</td>
<td>5</td>
</tr>
<tr>
<td>Gatekeeper</td>
<td>10.9.5</td>
<td>Apple Inc.</td>
<td>Antimalware</td>
<td>windows 8 64-bit, mac osx 10.10</td>
<td>3</td>
</tr>
<tr>
<td>Software Update</td>
<td>2.3</td>
<td>Apple Inc.</td>
<td>Patch Management</td>
<td>windows 7 64-bit, mac osx 10.10, mac osx 8, mac osx 9</td>
<td>5</td>
</tr>
</tbody>
</table>

Click an endpoint in the **Endpoints With This Software** column in the table to view the endpoint details, such as Mac address, NAD IP address, NAD port ID/SSID, IPv4 address, and so on.

You can select an application name and choose the **Create App Compliance** option from the **Policy Actions** drop-down list to create application compliance condition and remediation.

---

**The Hardware Dashboard**

The endpoint hardware tab under context visibility helps you collect, analyze, and report endpoint hardware inventory information within a short time. You can gather information, such as finding endpoints with low memory capacity or finding the BIOS model/version in an endpoint. You can increase the memory capacity...
or upgrade the BIOS version based on these findings. You can assess the requirements before you plan the purchase of an asset. You can ensure timely replacement of resources. You can collect this information without installing any modules or interacting with the endpoint. In summary, you can effectively manage the asset lifecycle.

The Context Visibility > Endpoints > Hardware page displays the Manufacturers and Endpoint Utilizations dashlets. These dashlets reflect the changes based on the selected filter. The Manufacturers dashlet displays hardware inventory details for endpoints with Windows and Mac OS. The Endpoint Utilizations dashlet displays the CPU, Memory, and Disk utilization for endpoints. You can select any of the three options to view the utilization in percentage.

- Devices With Over n% CPU Usage.
- Devices With Over n% Memory Usage.
- Devices With Over n% Disk Usage.

The hardware inventory data takes 120 seconds to be displayed in the ISE GUI. The hardware inventory data is collected for posture compliant and non-compliant states.

The hardware attributes of an endpoint and their connected external devices are displayed in a table format. The following hardware attributes are displayed:

- MAC Address
- BIOS Manufacturer
- BIOS Serial Number
- BIOS Model
- Attached Devices
- CPU Name
- CPU Speed (GHz)
- CPU Usage (%)
- Number of Cores
- Number of Processors
- Memory Size (GB)
- Memory Usage (%)
- Total Internal Disk(s) Size (GB)
- Total Internal Disk(s) Free Size (GB)
- Total Internal Disk(s) Usage (%)
- Number of Internal Disks
- NAD Port ID
- Status
Cisco Identity Services Engine Administrator Guide, Release 2.2

Filtering Displayed Data in a View

Clicking any of the dashlets on a Context Visibility page filters the data that is displayed by the item you clicked, for example, a section of a pie chart.
If you click **mobil...vices** in the Endpoints dashlet, the page redispalyes with two Endpoints dashlets, a Network Devices dashlet, and a list of data. The dashlets and list show data for mobile devices, as shown in the following example:

You can continue to filter data by clicking more sections of the pie charts, or by using the controls on the list of data.
1. The gear icon filters the displayed columns. The drop-down lets you choose which columns to display in this dashboard’s list.

2. The Quick filter is displayed by default. Entering characters into the box (label number 3) filters the list based on the result. The Custom Filter provides a more granular filter, as shown below.

You can save your custom filters.

**Endpoint Actions in a View’s List**

The toolbar at the top of the list allows you to take actions on endpoints in the list that you selected. Not all actions are enabled for every list, some actions depend on a feature being enabled for use. The following list shows two endpoint actions that must be enabled in ISE before you can use them.

- If Adaptive Network Control (ANC) is enabled, you can select endpoints in the list, and assign or revoke network access. You can also issue a change of authorization (CoA):
ANC (Endpoint Protection Services) is enabled in ISE under Administration > System > Settings > Endpoint Protection Service > Adaptive Network Control. For more information, see Enable Adaptive Network Control in Cisco ISE, on page 299.

- If MDM is installed, you can perform MDM actions on selected endpoints.

Attributes in Context Visibility

The systems and services that provide attributes for Context Visibility sometimes have different values for the same attribute name. A few examples are shown below:

**For Operating System**
- OperatingSystem—Posture operating system
- operating-system—NMAP operating system
- operating-system-result—Profiler consolidated operating system

**For Portal Name**
- Portal.Name—Guest portal name when device registration is turned on
- PortalName—Guest portal name when device registration is not turned on

**Portal User**
- User-Name—User name from RADIUS authentication
- GuestUserName—Guest user
- PortalUser—Portal user

Cisco ISE Internationalization and Localization

Cisco ISE internationalization adapts the user interface for supported languages. Localization of the user interface incorporates locale-specific components and translated text. For Windows, MAC OSX, and Android devices, the native supplicant provisioning wizard can be used in any of the following supported languages.

In Cisco ISE, internalization and localization support focuses on support for non-English text in UTF-8 encoding to the end-user facing portals and on selective fields in the Admin portal.

**Supported Languages**

Cisco ISE, provides localization and internalization support for the following languages and browser locales:

<table>
<thead>
<tr>
<th>Language</th>
<th>Browser Locale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chinese traditional</td>
<td>zh-tw</td>
</tr>
<tr>
<td>Chinese simplified</td>
<td>zh-cn</td>
</tr>
<tr>
<td>Czech</td>
<td>cs-cz</td>
</tr>
</tbody>
</table>
End-User Web Portal Localization

The Guest, Sponsor, My Devices, and Client Provisioning portals are localized into all supported languages and locales. This includes text, labels, messages, field names, and button labels. If the client browser requests a locale that is not mapped to a template in Cisco ISE, the portals display content using the English template.

Using the Admin portal, you can modify the fields used for the Guest, Sponsor, and My Devices portals for each language individually, and you can add additional languages. Currently, you cannot customize these fields for the Client Provisioning portal.

You can further customize the Guest portal by uploading HTML pages to Cisco ISE. When you upload customized pages, you are responsible for the appropriate localization support for your deployment. Cisco ISE provides a localization support example with sample HTML pages, which you can use as a guide. Cisco ISE provides the ability to upload, store, and render custom internationalized HTML pages.

Note

NAC and MAC agent installers and WebAgent pages are not localized.

Support for UTF-8 Character Data Entry

Cisco ISE fields that are exposed to the end user (through the Cisco NAC agent, or supplicants, or through the Sponsor, Guest, My Devices, and Client Provisioning portals) support UTF-8 character sets for all languages. UTF-8 is a multibyte-character encoding for the unicode character set, which includes many different language character sets, such as Hebrew, Sanskrit, and Arabic.
Character values are stored in UTF-8 in the administration configuration database, and the UTF-8 characters display correctly in reports and user interface components.

**UTF-8 Credential Authentication**

Network access authentication supports UTF-8 username and password credentials. This includes RADIUS, EAP, RADIUS proxy, RADIUS token, and web authentication from the Guest and Administrative portal login authentications. UTF-8 support for username and password applies to authentication against the local identity store as well as external identity stores.

UTF-8 authentication depends on the client supplicant that is used for network login. Some Windows native supplicants do not support UTF-8 credentials.

---

**Note**

RSA does not support UTF-8 users, hence UTF-8 authentication with RSA is not supported. Likewise, RSA servers, which are compatible with Cisco ISE, do not support UTF-8.

---

**UTF-8 Policies and Posture Assessment**

Policy rules in Cisco ISE that are conditioned on attribute values may include UTF-8 text. Rule evaluation supports UTF-8 attribute values. In addition, you can configure conditions with UTF-8 values through the Administrative portal.

Posture requirements can be modified as File, Application, and Service conditions based on a UTF-8 character set. This includes sending UTF-8 requirement values to the NAC agent. The NAC agent then assesses the endpoint accordingly, and reports UTF-8 values, when applicable.

---

**UTF-8 Support for Messages Sent to Supplicant**

RSA prompts and messages are forwarded to the supplicant using a RADIUS attribute REPLY-MESSAGE, or within EAP data. If the text contains UTF-8 data, it is displayed by the supplicant, based on the client’s local operating system language support. Some Windows-native supplicants do not support UTF-8 credentials.

Cisco ISE prompts and messages may not be in sync with the locale of the client operating system on which the supplicant is running. You must align the end-user supplicant locale with the languages that are supported by Cisco ISE.

---

**Reports and Alerts UTF-8 Support**

Monitoring and troubleshooting reports and alerts support UTF-8 values for relevant attributes, for Cisco ISE supported languages, in the following ways:

- Viewing live authentications
- Viewing detailed pages of report records
- Exporting and saving reports
- Viewing the Cisco ISE dashboard
- Viewing alert information
- Viewing tcpdump data
UTF-8 Character Support in the Portals

Many more character sets are supported in Cisco ISE fields (UTF-8) than are currently supported for localizations in portals and end-user messages. For example, Cisco ISE does not support right-to-left languages, such as Hebrew or Arabic, even though the character sets themselves are supported.

The following table lists the fields in the Admin and end-user portals that support UTF-8 characters for data entry and viewing, with the following limitations:

• Cisco ISE does not support guest usernames and passwords with UTF-8 characters.
• Cisco ISE does not support UTF-8 characters in certificates.

Table 2: Admin Portal UTF-8 Character Fields

<table>
<thead>
<tr>
<th>Admin Portal Element</th>
<th>UTF-8 Fields</th>
</tr>
</thead>
</table>
| Network access user configuration | • User name  
                               | • First name  
                               | • Last name  
                               | • e-mail  |
| User list                     | • All filter fields  
                               | • Values shown on the User List page  
                               | • Values shown on the left navigation quick view  |
| User password policy          | The passwords can be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(”, and “)”). Password field accepts any characters including UTF-8 characters, but it doesn't accept control characters.  
                               | Some languages do not have uppercase or lowercase alphabets. If your user password policy requires the user to enter a password with uppercase or lowercase characters, and if the user’s language does not support these characters, the user cannot set a password. For the user password field to support UTF-8 characters, in the user password policy page (Administration > Identity Management > Settings > User Password Policy), you must uncheck the following options:  
                               | • Lowercase alphabetic characters  
<pre><code>                           | • Uppercase alphabetic characters  |
</code></pre>
<table>
<thead>
<tr>
<th>Admin Portal Element</th>
<th>UTF-8 Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator list</td>
<td>• All filter fields</td>
</tr>
<tr>
<td></td>
<td>• Values shown on the Administrator List page</td>
</tr>
<tr>
<td></td>
<td>• Values shown on the left navigation quick view</td>
</tr>
<tr>
<td>Admin login page</td>
<td>• User name</td>
</tr>
<tr>
<td>RSA</td>
<td>• Messages</td>
</tr>
<tr>
<td></td>
<td>• Prompts</td>
</tr>
<tr>
<td>RADIUS token</td>
<td>• Authentication tab &gt; Prompt</td>
</tr>
<tr>
<td>Posture Requirement</td>
<td>• Name</td>
</tr>
<tr>
<td></td>
<td>• Remediation action &gt; Message shown to Agent User</td>
</tr>
<tr>
<td></td>
<td>• Requirement list display</td>
</tr>
<tr>
<td>Posture conditions</td>
<td>• File condition &gt; File path</td>
</tr>
<tr>
<td></td>
<td>• Application condition &gt; Process name</td>
</tr>
<tr>
<td></td>
<td>• Service condition &gt; Service name</td>
</tr>
<tr>
<td></td>
<td>• Conditions list display</td>
</tr>
<tr>
<td>Guest and My Devices settings</td>
<td>• Sponsor &gt; Language Template: all supported languages, all fields</td>
</tr>
<tr>
<td></td>
<td>• Guest &gt; Language Template: all supported languages, all fields</td>
</tr>
<tr>
<td></td>
<td>• My Devices &gt; Language Template: all supported languages, all fields</td>
</tr>
<tr>
<td>System settings</td>
<td>• SMTP Server &gt; Default e-mail address</td>
</tr>
<tr>
<td>Operations &gt; Alarms &gt; Rule</td>
<td>• Criteria &gt; User</td>
</tr>
<tr>
<td></td>
<td>• Notification &gt; e-mail Notification user list</td>
</tr>
<tr>
<td>Operations &gt; Reports</td>
<td>• Operations &gt; Live Authentications &gt; Filter fields</td>
</tr>
<tr>
<td></td>
<td>• Operations &gt; Reports &gt; Catalog &gt; Report filter fields</td>
</tr>
<tr>
<td>Operations &gt; Troubleshoot</td>
<td>• General Tools &gt; RADIUS Authentication Troubleshooting &gt; Username</td>
</tr>
</tbody>
</table>
UTF-8 Support Outside the User Interface

This section contains the areas outside the Cisco ISE user interface that provide UTF-8 support.

Debug Log and CLI-Related UTF-8 Support

Attribute values and posture condition details appear in some debug logs; therefore, all debug logs accept UTF-8 values. You can download debug logs containing raw UTF-8 data that can be viewed with a UTF-8 supported viewer.

ACS Migration UTF-8 Support

Cisco ISE, allows for the migration of ACS UTF-8 configuration objects and values. Migration of some UTF-8 objects may not be supported by Cisco ISE UTF-8 languages, which might render some of the UTF-8 data that is provided during migration as unreadable using Administrative portal or report methods. You must convert unreadable UTF-8 values (that are migrated from ACS) into ASCII text. For more information about migrating from ACS to ISE, see the Cisco Secure ACS to Cisco ISE Migration Tool for your version of ISE.

Support for Importing and Exporting UTF-8 Values

The Admin and Sponsor portals support plain text and .csv files with UTF-8 values to be used when importing user account details. Exported files are provided as csv files.
UTF-8 Support on REST

UTF-8 values are supported on external REST communication. This applies to configurable items that have UTF-8 support in the Cisco ISE user interface, with the exception of admin authentication. Admin authentication on REST requires ASCII text credentials for login.

UTF-8 Support for Identity Stores Authorization Data

Cisco ISE allows Active Directory and LDAP to use UTF-8 data in authorization policies for policy processing.

MAC Address Normalization

ISE supports normalization of MAC address entered by you in any of the following formats:

- 00-11-22-33-44-55
- 0011.2233.4455
- 00:11:22:33:44:55
- 001122334455
- 001122-334455

For the following ISE windows, you can provide full or partial MAC address:

- Policy > Policy Sets
- Policy > Policy Elements > Conditions > Authorization
- Authentications > Filters (Endpoint and Identity columns)
- Global Search
- Operations > Reports > Reports Filters
- Operations > Diagnostic Tools > General Tools > Endpoint Debug

For the following ISE windows, you should provide full MAC address (six octets separated by ‘:’ or ‘-’ or ‘.’):

- Operations > Endpoint Protection Services Adaptive Network Control
- Operations > Troubleshooting > Diagnostic Tools > General Tools > RADIUS Authentication Troubleshooting
- Operations > Troubleshooting > Diagnostic Tools > General Tools > Posture Troubleshooting
- Administration > Identities > Endpoints
- Administration > System > Deployment
- Administration > Logging > Collection Filter

REST APIs also support normalization of full MAC address.

Valid octet can contain only 0-9, a-f or A-F.
Admin Features Limited by Role-Based Access Control Policies

Cisco ISE provides role-based access control (RBAC) policies that ensure security by restricting administrative privileges. RBAC policies are associated with default admin groups to define roles and permissions. A standard set of permissions (for menu as well as data access) is paired with each of the predefined admin groups, and is thereby aligned with the associated role and job function.

Some features in the user interface require certain permissions for their use. If a feature is unavailable, or you are not allowed to perform a specific task, your admin group may not have the necessary permissions to perform the task that utilizes the feature.

Regardless of the level of access, any administrator account can modify or delete objects for which it has permission, on any page that it can access.
What Is Wireless Setup

Wireless Setup provides an easy way to set up wireless flows for 802.1x, guest, and BYOD. It also provides workflows to configure and customize each portal for guest and BYOD, where appropriate. These workflows are much simpler than configuring the associated portal flow in ISE by providing the most common recommended settings. Wireless Setup does many steps for you that you would have to do yourself in ISE, and on the WLC, so you can quickly create a working environment.

You can use the Wireless Setup created environment to test and develop your flows. Once you get your Wireless Setup environment working, you may want to switch to ISE, so you can support more advanced configurations. For more information about configuring Guest in ISE, see the ISE Administrators Guide for your version of ISE, and the Cisco Community Site https://communities.cisco.com/docs/DOC-64018. For more information about configuring and using Wireless Setup for ISE, see https://communities.cisco.com/docs/DOC-71189.


- **Wireless Setup is disabled** by default after fresh installation of Cisco ISE. You can enable Wireless Setup from the ISE CLI with the `application configure ise` command (select option 17) or by using the Wireless Setup option in the ISE GUI Home page.

- Wireless Setup does not work if you upgrade ISE from a previous version. Wireless Setup is supported only for new ISE installations.

- Wireless Setup works only on a Standalone node.

- Run only one instance of Wireless Setup at a time; only one person can run Wireless Setup at a time.

- Wireless Setup requires ports 9103 and 9104 to be open. To close those ports, use the CLI to disable Wireless Setup.

- If you would like to start a fresh installation of Wireless Setup after running some flows, you can use the CLI command `application reset-config ise`. This command resets the ISE configuration and clears the ISE database, but keeps the network definitions. So you can reset ISE and Wireless Setup, without having to reinstall ISE and running setup.

  If you would like to start over with Wireless Setup, you can reset both ISE and Wireless Setup's configuration with the following steps:
• In the CLI, run application reset-config to reset all ISE configuration. If you were testing Wireless Setup on a fresh installation, this command removes the configurations done by Wireless Setup in ISE.

• In the CLI, run application configure ise, and choose [18]Reset Config Wi-Fi Setup. This cleans the Wireless Setup configuration database.

• On the WLC, remove the configurations added by Wireless Setup on the WLC. For information about what Wireless Setup configures on the WLC, see Changes to ISE and WLC by Wireless Setup, on page 42.

You can avoid these steps by taking a snapshot of the VM after you finish a fresh installation of ISE. For more information about the CLI, see the Cisco Identity Services Engine CLI Reference Guide for your version of ISE.

• You must be an ISE Super Admin user to use Wireless Setup.

• Wireless Setup requires at least two CPU cores and 8 GB or memory.

• Only Active Directory groups and users are supported. After you have created one or more flows in Wireless Configuration, other types of users, groups, and authorizations are available for Wireless Setup, but they must be configured on ISE.

• If you already defined Active Directory in ISE, and you plan to use this AD for Wireless Setup, then:
  • The join name and domain name must be the same. If the names are not the same, then make them the same in ISE before using that AD in Wireless Setup.
  • If your WLC is already configured on ISE, the WLC must have a shared secret configured. If the WLC definition does not have the shared secret, then either add the shared secret, or delete the WLC from ISE, before configuring that WLC in Wireless Setup.

• Wireless Setup can configure ISE components, but it can't delete or modify them after a flow has been started. For a list of all the things that Wireless Setup configures in ISE, see Cisco Identity Services Engine CLI Reference Guide for your version of ISE.

• When you start a flow, you must complete the flow. Clicking a breadcrumb in the flow stops the flow. As you step through a flow, changes are made to the ISE configuration dynamically. Wireless Setup provides a list of configuration changes, so you can manually revert. You can't back up in a flow to make extra changes, with one exception. You can go back to change Guest or BYOD portal customization.

• Multiple WLCs and Active Directory domains are supported, but each flow can only support one WLC and one Active Directory.

• Wireless Setup requires an ISE Basic license to operate. BYOD requires a Plus license.

• If you have configured ISE 2.2 resources before configuring Wireless Setup, Wireless Setup may have conflicts with an existing policy. If this happens, Wireless Setup advises you to review the authorization policy after running through the tool. We recommended that you start with a clean setup of ISE when running Wireless Setup. Support for a mixed configuration of Wireless Setup and ISE is limited.

• Wireless Setup is available in English, but not other languages. If you want to use other languages with your portal, configure that in ISE after running Wireless Setup.
• Dual SSID is supported for BYOD. The Open SSID used in this configuration does not support guest access, due to conflicts. If you need a portal that supports both guest and BYOD, you cannot use Wireless Setup, and is out of the scope of this document.

• Email and SMS Notifications
  • For self-registered guests, SMS and email notification is supported. These notifications are configured in the portal customization notification section. You must configure an SMTP server to support SMS and email notifications. The cellular providers built in to ISE, which include AT&T, T Mobile, Sprint, Orange and Verizon, are pre-configured, and are free email to SMS gateways.
  • A guest chooses their cell provider in the portal. If their provider is not in the list, then they can't receive a message. You can also configure a global provider, but that is outside of the scope of this guide. If the guest portal is configured for SMS and email notification, then they must enter values for both those services.
  • The Sponsored guest flow does not provide configuration for SMS or email notification in Wireless Setup. For that flow, you must configure notification services in ISE.
  • Do not select the SMS provider Global Default when configuring notifications for a portal. This provider is not configured (by default).

• Wireless setup only supports a standalone setup without HA. If you decide to use extra PSNs for authentication, then add the ISE IP address of those PSNs to your WLC’s RADIUS configuration.

Wireless Setup Support for Apple Mini-Browser (Captive Network Assistant)
• Guest Flows — Auto popup of the Apple pseudo browser works with all Guest Flows. A guest may go through the flow using Apple's Captive Network Assistant browser. When an Apple user connects to the OPEN network, the minibrowser pops-up automatically, which allows them to accept an AUP (hotspot), or to go through self-registration or login with their credentials.

• BYOD
  • Single SSID — ISE 2.2 added support for the apple minibrowser. However, to limit potential problems with SSID flows on Apple devices, we suppressed the minibrowser by adding captive.apple.com to the redirection ACL. This causes the Apple device to think it has access to the Internet. The user must manually launch Safari to be redirected to the portal for web authentication or device onboarding.
  • Dual SSID — For Dual SSID flow that starts with an initial OPEN network WLAN to start guest access, or to allow your employees to go through Device Onboarding (BYOD), and redirects to a secured SSID, the minibrowser is also suppressed.

For more information about the Apple CAN minibrowser, see https://communities.cisco.com/docs/DOC-71122.
Configuring WLCs in Wireless Network

When you first log on to Wireless Setup and select a flow, you are asked to configure a wireless controller. Wireless Setup pushes the necessary settings to the WLC to support the type of flow you are configuring.

- The WLC must be a Cisco WLC running AireOS 8.x or higher.
- vWLC doesn’t support DNS based ACLs
- Configure your WLC for the interface VLANS (networks) that you plan to use in your Wireless Setup deployment. By default, the WLC has a management interface, but we recommend that you configure other interfaces for your guest and secure access (employee) networks.
- For Guest flow, an ACL_WEBAUTH_REDIRECT ACL is used to redirect guest devices to either a Hotspot or Credentialed Portal to acceptance of an AUP (hotspot), to log in, or to create credentials. After the Guest is authorized, they are permitted access (ACCESS-ACCEPT). You can use ACLs on the WLC to restrict guest permissions: create an ACL on the WLC, and use that ACL in your guest permission authz profile. To allow access to the ISE success page, add this ACL to the WLC. For more information about creating restrictive ACLs, see https://communities.cisco.com/docs/DOC-68169.
- Wireless Setup configures a WLAN for each flow. Once you have configured a WLAN for a flow, that WLAN is not available for any other flow. The only exception to this is if you configured a WLAN for self-registration flow, and later you decided to use this WLAN for a Sponsored Guest Flow, which handles both self-registration and sponsoring of guests.

If you run Wireless Setup in a production environment, your configurations may disconnect some existing users.

- If you configure a flow in Wireless Setup with a WLC, do not remove that WLC in ISE.
- If you have already configured a WLC in ISE, but you didn't configure a shared secret in the RADIUS Options, then you must add a shared secret before using that WLC in Wireless Setup.
- If you already configured a WLC in ISE, and you configured a shared secret, then don't configure a different shared secret with Wireless Setup. The Wireless Setup and the ISE secret passwords must match. The WLAN that you select is disabled throughout the flow, but it can be re-enabled at the end of the flow by clicking the Go Live button.
- Remote LAN—If your network has a remote LAN, Wireless Setup fails when it tries to use a VLAN ID that is already assigned to your remote LAN. To work around this, either remove the remote LAN, or create the VLANs that you plan to use on the WLC before you run Wireless Setup. In Wireless Setup, you can enable those existing VLANs for flows.
- FlexConnect—Flexconnect Local Switch and Flexconnect ACLs are configured by Wireless Setup, but they are not used or supported. Wireless Setup only works with Flexconnect Centralized or Local Mode Aps and SSIDs.

Example of Wireless Configuration

The following extraction from a WLC log shows an example of the configuration that Wireless Setup does when you configure a flow.
Active Directory with Wireless Setup

An Active Directory Domain is required to create Sponsored Guest, 802.1x, and BYOD flows. Active Directory identifies users for the sponsor groups to access the Sponsor portal, 802.1x Secure Access and associated VLANs, and BYOD and device onboarding. After configuring any of these flows in Wireless Setup, you can optionally go into ISE Identities and add:

- A internal sponsor account mapped to sponsor group, such as ALL_ACCOUNTS. This is not required if you are using Active Directory.
- An employee who is part of the ISE internal employee group. Make sure that the internal Employee group is added to your Authorization Policy and ISE internal employee group.
Guest Portals in Wireless Setup

When people visiting your company wish to use your company’s network to access the internet, or resources and services on your network, you can provide them network access through a Guest portal. Employees can use these Guest portals to access your company’s network, if configured.

There are three default Guest portals:

- **Hotspot Guest portal**—Network access is granted without requiring any credentials. Usually, an Acceptance of User Policy (AUP) must be accepted before network access is granted.

- **Sponsored-Guest portal**—Network access is granted by a sponsor who creates accounts for guests, and provides the Guest with login credentials.

- **Self-Registered Guest portal**—Guests can create their own accounts credentials, and may need sponsor approval before they are granted network access.

Cisco ISE can host multiple Guest portals, including a predefined set of default portals.

The default portal themes have standard Cisco branding that you can customize through the Admin portal.

Wireless setup has its own default theme (CSS) and you are able to modify some basic settings such as logo, banner, background image, coloring and fonts. In ISE, you can also choose to further customize your portal by changing more settings and go into advanced customizations.

**Guest Portal Workflow**

1. After you choose the type of portal, you are asked which controller to use. Configure a new wireless network for each flow. You can choose an existing WLAN that you haven’t already used in Wireless Setup, or create a new one.

   Flows that require redirection have the option of redirecting the user to an Originating URL, success page, or specific URL (for example, www.cisco.com). Originating URL requires support from the WLC.

   **Note**
   
   Originating URL is not supported until WLC version 8.4 is release.

2. Customize the appearance and change the basic settings of the portal.

3. When you're done with customization, follow the URL link to the test portal. The test portal shows you a preview of a test version of the portal. You can continue through the flow, and make more changes, if desired. Note, the only success redirection that works in the preview portal is to the Success Page. Original URL and Static URL do not work, since they require a wireless session to support the redirect.

4. Configuration is done. You can download and view the steps that Wireless Setup did for you in ISE and the WLC during the workflow.

   **Note**
   
   Location is not used for basic guest access in Wireless Setup. Locations are required if you want to control access based on local time. For information about configuring time zones in ISE, see SMS Providers and Services, on page 455.
**Wireless Network Self-Registration Portal**

A Self-Registered Guest portal enables guests to register themselves and create their own accounts so they can access the network.

We recommend that you do not choose logon success page, which displays logon credentials to the user on screen. The best practice is to require the user to get their credentials via email or SMS, which associates them with something unique for audit purposes.

**Wireless Network Sponsored Guest Flow**

Sponsors use the Sponsor portal to create and manage temporary accounts for authorized visitors to securely access the corporate network or the Internet. After creating a guest account, sponsors can also use the Sponsor portal to provide account details to the guest by printing, emailing, or texting. Before providing self-registering guests access to the company network, sponsors may be requested via email to approve their guests’ accounts.

Wireless Setup configures a sponsor portal and a sponsored guest portal during the sponsored flow.

Approval flow is not supported with Wireless Setup.

You map Active Directory groups to your Sponsor Groups during the workflow. The workflow maps the AD Groups you select to the ALL_ACCOUNTS Sponsor group. It does not configure the GROUP or OWN account sponsor groups. Optionally, if you want to add other identity sources (such as internal or LDAP settings) you may do this in the ISE admin UI. For more information, see Sponsor Groups.

**Wireless Setup BYOD Flow - For Native Supplicant and Certificate Provisioning**

The Bring Your Own Device (BYOD) portal enables employees to register their personal devices. Native supplicant and certificate provisioning can be done before allowing access to the network. Employees do not access the BYOD portal directly, they are redirected to this portal when registering personal devices. The first time employees attempt to access the network using a personal device, they may be prompted to manually download (for non-iOS devices) and launch the Network Setup Assistant (NSA) wizard. The NSA guides them through registering and installing the native supplicant. After they have registered a device, they can use the My Devices portal to manage it.

Wireless Setup configures ISE and the controller for native supplicant and certificate provisioning. The user makes a PEAP connection to the controller, provides credentials, and the connection is switched to EAP-TLS (certificate).

The following devices are supported with Wireless setup: Apple Devices (MAC and iOS), Windows Desktop OS (but not mobile), and Android. Chrome OS on boarding is not supported by Wireless Setup.
Dual SSID flow consists of an open network for onboarding, and a TLS certificate-based secure network for authenticated access. A device can connect to the secure network without onboarding. This is because the basic_authenticated_access default rule allows any valid authentication to pass. When the device connects to the secure network, they don’t match the BYOD secured authorization rule, the match falls to the bottom of the list to basic_authenticated_access.

The fix is to disable the Basic_Authenticated_Access rule under authorization policies, or edit the rule to match a specific SSID (WLAN). Both changes block PEAP connections to those that shouldn’t allow it.

Wireless Setup does not have an authorization rule to redirect devices that are marked as lost. This is called blacklisting, which is managed by the blacklist portal. For information about managing lost and stolen devices, see http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Borderless_Networks/Unified_Access/BYOD_Design_Guide/Managing_Lost_or_Stolen_Device.pdf.

BYOD Flow in Wireless Setup

BYOD Configuration in Wireless Setup consists of the following steps:

1. Choosing or Registering a wireless LAN controller
2. Adding a wireless network: For Dual SSID, this step runs twice.

A new ISE installation includes a default wireless network. With dual SSID BYOD, when the user is redirected to the second SSID, they will also see the default network SSID in their network profile. You can delete the default SSID, or tell your users to ignore it.

3. Choosing or joining an Active Directory (AD): You can override default VLAN settings for both the onboarding VLAN and the final access VLAN. The final access VLAN is mapped to the Active Directory groups.
4. Customizing your BYOD Portals: You can customize BYOD and My Devices Portal here. You can customize all the pages that ISE supports in this step. In this step, all the portal customization is submitted, policies are created and the profiles are linked to the respective policies.

My Devices portal uses the basic customization from BYOD portal customization; you cannot customize My Devices portal in Wireless Setup.

5. Preview the configuration changes made, and select Done.

For Dual SSID BYOD

Fast SSID must be enabled to support dual SSID BYOD. When Fast SSID changing is enabled, the wireless controller allows clients to move faster between SSIDs. When fast SSID is enabled, the client entry is not
cleared and the delay is not enforced. For more information about configuring Fast SSID on a Cisco WLC, see the Cisco Wireless Controller Configuration Guide.

**Recommended WLC Timer Settings**

We recommend setting the following timers on the WLC that you plan to use with Wireless Setup. The settings are shown in CLI.

```
config radius auth retransmit-timeout (SERVER_INDEX) 5
config radius aggressive-failover disable
config radius fallback-test mode passive
config wlan exclusionlist (WLAN ID) 180
config wlan exclusionlist (WLAN ID) enabled
```

**Secure Access Flow**

Wireless Setup flow configures an 802.1x Wireless LAN controller for PEAP (username and password credentials).

Part of the flow asks you to specify an Active Directory (AD). You can map employee AD groups to a VLAN. You can configure different employee groups to different VLANs, if you want to separate your groups by VLAN. Click the drop-down next to **access** to see the AD groups available in the AD you configured.

Using Secure Access with Active Directory, if you don't map and AD group to a VLAN, then the user matches the basic access policy, which allows any valid AD user to login. If you choose AD groups in Wireless Setup, each group is mapped to VLAN.

**Employee Connects to Network**

1. **Employee Credentials Are Authenticated** — Cisco ISE authenticates the employee against the corporate Active Directory and provides an authorization policy.

2. **Device Is Redirected to the BYOD Portal** — The device is redirected to the BYOD portal. The device’s MAC address is automatically preconfigured, and the user can add a device name and description.

3. **Native Supplicant Is Configured (MacOS, Windows, iOS, Android)** — The native supplicant is configured; but the process varies by device:
   - MacOS and Windows devices — Employee clicks **Register** in the BYOD portal to download and install the supplicant provisioning wizard, which configures the supplicant and installs the certificate used for EAP-TLS certificate based authentication. The issued certificate is embedded with the device’s MAC address and employee's username.
   - iOS devices — The Cisco ISE policy server sends a new profile using Apple’s iOS over the air to the IOS device, which includes:
     - The issued certificate is embedded with the IOS device's MAC address and employee's username.
     - A Wi-Fi supplicant profile that enforces the use of MSCHAPv2 or EAP-TLS for 802.1X authentication.
   - Android devices — Cisco ISE prompts and routes employee to download the Cisco Network Setup Assistant (NSA) from the Google Play store. After installing the app, the employee can open NSA and start the setup wizard, which generates the supplicant configuration and issued certificate used to configure the device.
• **Change of Authorization Issued**—After the user goes through the on boarding flow, Cisco ISE initiates a Change of Authorization (CoA). This causes the MacOS X, Windows, and Android devices to reconnect to the secure 802.1X network using EAP-TLS. For single SSID, iOS devices also connect automatically, but for dual SSID, the wizard prompts iOS users to manually connect to the new network.

Native supplicants are supported for these operating systems:

- Android (excluding Amazon Kindle, B&N Nook)
- Mac OS X (for Apple Mac computers)
- Apple iOS devices (Apple iPod, iPhone, and iPad)
- Microsoft Windows 7, 8 (excluding RT), Vista, and 10

**Changes to ISE and WLC by Wireless Setup**

Wireless Setup configures ISE and the controller as you step through a flow. Wireless Setup lists the changes it made at the end of each flow. The changes for each flow are listed here as a reference to help you find all the changes that Wireless Setup made to ISE, to review or change them.

- **Hotspot**
  - Work Centers > Guest Access > Portals & Components > Guest Portals > Hotspot Portal
  - Work Centers > Guest Access > Policy Elements > Results > Authorization Profiles
  - Work Centers > Guest Access > Policy Sets

- **Self-Registration**
  - Work Centers > Guest Access > Portals & Components > Guest Portals > Self-reg Portal
  - Work Centers > Guest Access > Portals & Components > Guest Types > Guest Types
  - Policy > Policy Elements > Authorization > Authorization Profiles
  - Work Centers > Guest Access > Policy Sets
  - Administration > System > Settings > SMTP Server
  - Administration > System > Settings > SMTP Gateway

- **Sponsored**
  - Work Centers > Guest Access > Portals & Components > Guest Portals > Sponsored Guest Portal
  - Work Centers > Guest Access > Portals & Components > Sponsor Portals > > Sponsor Portal
  - Policy > Policy Elements > Authorization > Authorization Profiles
  - Work Centers > Guest Access > Authorization Policy
• Work Centers > Guest Access > Portals & Components > Sponsor > Sponsor Groups
• Work Centers > Guest Access > Portals & Components > Guest Types > Guest Types
• Work Centers > Guest Access > Ext ID Sources > Active Directory

• BYOD
  • Work Centers > BYOD > Portals & Components > BYOD Portals > BYOD Portal
  • Work Centers > BYOD > Portals & Components > My Devices Portals > My Devices Portal
  • Work Centers > BYOD > Policy Elements > Authorization > Authorization Profiles
  • Work Centers > BYOD > Authorization Policy
  • Work Centers > BYOD > Ext ID Sources > Active Directory
  • Work Centers > BYOD > Ext ID Sources > Active Directory, then select your AD, then the Groups tab.

• Secure Access
  • Policy > Policy Elements > Results > Authorization > Authorization Profiles
  • Policy > Policy Sets
  • Work Centers > Guest Access > Ext ID Sources > Active Directory, then select your AD, then the Groups tab.

• Wireless LAN Controller
  • WLANs
    • Security > Access Control Lists—Wireless Setup creates the following ACL:
      • Redirect ACL for guest and BYOD

    • Wireless setup also creates entries under Security > AAA > Authentication and Accounting
PART II

Deploy Cisco ISE Nodes

• Set Up Cisco ISE in a Distributed Environment, on page 47
Chapter 4

Set Up Cisco ISE in a Distributed Environment

- Cisco ISE Deployment Terminology, on page 47
- Personas in Distributed Cisco ISE Deployments, on page 48
- Cisco ISE Distributed Deployment, on page 48
- Configure a Cisco ISE Node, on page 51
- Administration Node, on page 54
- Policy Service Node, on page 61
- Monitoring Node, on page 62
- pxGrid Node, on page 64
- View Nodes in a Deployment, on page 68
- Synchronize Primary and Secondary Cisco ISE Nodes, on page 68
- Change Node Personas and Services, on page 69
- Effects of Modifying Nodes in Cisco ISE, on page 69
- Create a Policy Service Node Group, on page 70
- Deploy pxGrid Node, on page 71
- Configure Monitoring Nodes for Automatic Failover, on page 71
- Remove a Node from Deployment, on page 72
- Change the Hostname or IP Address of a Standalone Cisco ISE Node, on page 73
- Replace the Cisco ISE Appliance Hardware, on page 73

Cisco ISE Deployment Terminology

The following terms are commonly used when discussing Cisco ISE deployment scenarios:

- Service—A service is a specific feature that a persona provides such as network access, profiler, posture, security group access, monitoring and troubleshooting, and so on.

- Node—A node is an individual instance that runs the Cisco ISE software. Cisco ISE is available as an appliance and also as a software that can be run on VMware. Each instance, appliance or VMWare that runs the Cisco ISE software is called a node.

- Persona—The persona or personas of a node determine the services provided by a node. A Cisco ISE node can assume any of the following personas: Administration, Policy Service, Monitoring, and pxGrid. The menu options that are available through the Admin portal are dependent on the role and personas that an Cisco ISE node assumes.
• Deployment Model—Determines if your deployment is distributed, standalone, or high availability in standalone, which is a basic two-node deployment.

**Personas in Distributed Cisco ISE Deployments**

A Cisco ISE node can assume the Administration, Policy Service, or Monitoring personas.

A Cisco ISE node can provide various services based on the persona that it assumes. Each node in a deployment can assume the Administration, Policy Service, and Monitoring personas. In a distributed deployment, you can have the following combination of nodes on your network:

- Primary and secondary Administration nodes for high availability
- A single or a pair of non-administration nodes for health check of Administration nodes for automatic failover
- A pair of health check nodes or a single health check node for PAN automatic failover
- One or more Policy Service nodes for session failover

**Cisco ISE Distributed Deployment**

A deployment that has more than one Cisco ISE node is called a distributed deployment. To support failover and to improve performance, you can set up your deployment with multiple Cisco ISE nodes in a distributed fashion. In Cisco ISE distributed deployment, administration and monitoring activities are centralized, and processing is distributed across the Policy Service nodes. Depending on your performance needs, you can scale your deployment. Each Cisco ISE node in a deployment can assume any of the following personas: Administration, Policy Service, and Monitoring.

**Cisco ISE Deployment Setup**

After you install Cisco ISE on all your nodes, as described in the *Cisco Identity Services Engine Hardware Installation Guide*, the nodes come up in a standalone state. You must then define one node as your Primary PAN. While defining your Primary PAN, you must enable the Administration and Monitoring personas on that node. You can optionally enable the Policy Service persona on the Primary PAN. After you complete the task of defining personas on the Primary PAN, you can then register other secondary nodes to the Primary PAN and define personas for the secondary nodes.

All Cisco ISE system and functionality-related configurations should be done only on the Primary PAN. The configuration changes that you perform on the Primary PAN are replicated to all the secondary nodes in your deployment.

There must be at least one Monitoring node in a distributed deployment. At the time of configuring your Primary PAN, you must enable the Monitoring persona. After you register a Monitoring node in your deployment, you can edit the Primary PAN and disable the Monitoring persona, if required.
Data Replication from Primary to Secondary ISE Nodes

When you register an Cisco ISE node as a secondary node, Cisco ISE immediately creates a data replication channel from the primary to the secondary node and begins the process of replication. Replication is the process of sharing Cisco ISE configuration data from the primary to the secondary nodes. Replication ensures consistency among the configuration data present in all Cisco ISE nodes that are part of your deployment.

A full replication typically occurs when you first register an ISE node as a secondary node. Incremental replication occurs after a full replication and ensures that any new changes such as additions, modifications, or deletions to the configuration data in the PAN are reflected in the secondary nodes. The process of replication ensures that all Cisco ISE nodes in a deployment are in sync. You can view the status of replication in the Node Status column from the deployment pages of the Cisco ISE Admin portal. When you register a Cisco ISE node as a secondary node or perform a manual synchronization with the PAN, the node status shows an orange icon indicating that the requested action is in progress. Once it is complete, the node status turns green indicating that the secondary node is synchronized with the PAN.

Cisco ISE Node Deregistration

To remove a node from a deployment, you must deregister it. When you deregister a secondary node from the Primary PAN, the status of the deregistered node changes to standalone and the connection between the primary and the secondary node will be lost. Replication updates are no longer sent to the deregistered standalone node.

When a PSN is deregistered, the endpoint data is lost. If you want the PSN to retain the endpoint data after it becomes a standalone node, you can do one of the following:

- Obtain a backup from the Primary PAN and when the PSN becomes a standalone node, restore this data backup on it.
- Change the persona of the PSN to Administration (Secondary PAN), synchronize the data from the deployment page of the Admin portal, and then deregister the node. This node will now have all the data. You can then add a secondary Admin node to the existing deployment.

Note

You cannot deregister a Primary PAN.

Guidelines for Setting Up a Distributed Deployment

Read the following statements carefully before you set up Cisco ISE in a distributed environment.

- Choose a node type, ISE node. For Administration, Policy Service, and Monitoring capabilities, you must choose an ISE node.
- Choose the same Network Time Protocol (NTP) server for all the nodes. To avoid timezone issues among the nodes, you must provide the same NTP server name during the setup of each node. This setting ensures that the reports and logs from the various nodes in your deployment are always synchronized with timestamps.
- Configure the Cisco ISE Admin password when you install Cisco ISE. The previous Cisco ISE Admin default login credentials (admin/cisco) are no longer valid. Use the username and password that was created during the initial setup or the current password if it was changed later.
• Configure the Domain Name System (DNS) server. Enter the IP addresses and fully qualified domain names (FQDNs) of all the Cisco ISE nodes that are part of your distributed deployment in the DNS server. Otherwise, node registration will fail.

• Configure the forward and reverse DNS lookup for all Cisco ISE nodes in your distributed deployment in the DNS server. Otherwise, you may run into deployment related issues when registering and restarting Cisco ISE nodes. Performance might be degraded if reverse DNS lookup is not configured for all the nodes.

• (Optional) Deregister a secondary Cisco ISE node from the Primary PAN to uninstall Cisco ISE from it.

• Back up the primary Monitoring node, and restore the data to the new secondary Monitoring node. This ensures that the history of the primary Monitoring node is in sync with the new secondary node as new changes are replicated.

• Ensure that the Primary PAN and the standalone node that you are about to register as a secondary node are running the same version of Cisco ISE.

Menu Options Available on Primary and Secondary Nodes

The menu options available in Cisco ISE nodes that are part of a distributed deployment depend on the personas that are enabled on them. You must perform all administration and monitoring activities through the Primary PAN. For other tasks, you must use the secondary nodes. Therefore, the user interface of the secondary nodes provides limited menu options based on the persona that are enabled on them.

If a node assumes more than one persona, for example, the Policy Service persona, and a Monitoring persona with an Active role, then the menu options listed for Policy Service nodes and Active Monitoring node will be available on that node.

The following table lists the menu options that are available on Cisco ISE nodes that assume different persona.

<table>
<thead>
<tr>
<th>Cisco ISE Node</th>
<th>Available Menu Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Nodes</td>
<td>• View and configure system time and NTP server settings.</td>
</tr>
<tr>
<td></td>
<td>• Install server certificate, manage certificate signing request. You can perform server certificate operations, for all the nodes in the deployment, via the Primary PAN that centrally manages all server certificates.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The private keys are not stored in the local database and are not copied from the relevant node; the private keys are stored in the local file system.</td>
</tr>
<tr>
<td>Primary PAN</td>
<td>All menus and sub-menus.</td>
</tr>
<tr>
<td>Cisco ISE Node</td>
<td>Available Menu Options</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active Monitoring Node</td>
<td>• Provides access to monitoring data (on both Primary and Active Monitoring nodes).</td>
</tr>
<tr>
<td></td>
<td>Note: The Operations menu can be viewed only from the Primary PAN. The Operations menu does not appear in the Monitoring nodes in Cisco ISE 2.1 and above.</td>
</tr>
<tr>
<td>Policy Service Nodes</td>
<td>Option to join, leave, and test Active Directory connection. Each Policy Service node must be separately joined to the Active Directory domain. You must first define the domain information and join the PAN to the Active Directory domain. Then, join the other Policy Service nodes to the Active Directory domain individually.</td>
</tr>
<tr>
<td>Secondary PAN</td>
<td>Option to promote the Secondary PAN to become the Primary PAN.</td>
</tr>
<tr>
<td></td>
<td>Note: After you have registered the secondary nodes to the Primary PAN, while logging in to the Admin portal of any of the secondary nodes, you must use the login credentials of the Primary PAN.</td>
</tr>
</tbody>
</table>

**Configure a Cisco ISE Node**

After you install a Cisco ISE node, all the default services provided by the Administration, Policy Service, and Monitoring personas run on it. This node will be in a standalone state. You must log in to the Admin portal of the Cisco ISE node to configure it. You cannot edit the personas or services of a standalone Cisco ISE node. You can, however, edit the personas and services of the primary and secondary Cisco ISE nodes. You must first configure a primary ISE node and then register secondary ISE nodes to the primary ISE node.

If you are logging in to the node for the first time, you must change the default administrator password and install a valid license.

It is recommended not to change the host name and the domain name on Cisco ISE that have been configured or in production. If it is required, then reimagine the appliance, make changes, and configure the details during the initial deployment.

**Before you begin**

You should have a basic understanding of how distributed deployments are set up in Cisco ISE. Read the guidelines for setting up a distributed deployment.

**Step 1** Choose Administration > System > Deployment.
Configure a Primary PAN

To set up a distributed deployment, you must first configure a Cisco ISE node as your Primary PAN.

**Step 1**  Choose Administration > System > Deployment.

The Register button will be disabled initially. To enable this button, you must configure a Primary PAN.

**Step 2**  Check the check box next to the current node, and click Edit.

**Step 3**  Click Make Primary to configure your Primary PAN.

**Step 4**  Enter data on the General Settings tab.

**Step 5**  Click Save to save the node configuration.

**What to do next**

1. Add secondary nodes to your deployment.

2. Enable the profiler service and configure the probes, if required.

Register a Secondary Cisco ISE Node

You can register ISE nodes to Primary PAN to form a multi-node deployment. Nodes in a deployment other than the Primary PAN are referred to as secondary nodes. While registering a node, you can select the personas and services that must be enabled on the node. Registered nodes can be managed from the Primary PAN (for example, managing the node personas, services, certificates, licenses, applying patches, and so on).

When a node is registered, Primary PAN will push the configuration data to the secondary node and the application server on the secondary node will restart. After this is complete, further configuration changes done on Primary PAN are replicated to the secondary node. The time taken for the changes to be replicated on the secondary node depends on various factors, such as the network latency, load on the system, and so on.

**Before you begin**

Ensure that the Primary PAN and the node being registered are DNS resolvable to each other. If the node being registered uses an untrusted self-signed certificate, you will be prompted with a certificate warning with the details of the certificate. If you accept the certificate, it will be added to the trusted certificate store of Primary PAN to enable TLS communication with the node. If the node uses a certificate that is not self-signed (for example, signed by external CA), you must manually import the relevant certificate chain of that node to the trusted certificate store of Primary PAN. When you import the secondary node's certificate in to the trusted certificate store, check the Trust for Authentication within ISE check box for the PAN to validate the secondary node's certificate.
While registering a node with session services enabled (such as Network Access, Guest, Posture, and so on), you can add it to a node group. Nodes that belong to the same node group share session information, thereby providing high availability and failover capabilities.

**Step 1**
Log into the Primary PAN.

**Step 2**
Choose **Administration** > **System** > **Deployment**.

**Step 3**
Click **Register** to initiate registration of a secondary node.

**Step 4**
Enter the DNS-resolvable fully qualified domain name (FQDN) of the standalone node that you are going to register (in the format hostname.domain-name, for example, abc.xyz.com). The FQDN of the Primary PAN and the node being registered must be resolvable from each other.

**Step 5**
Enter the UI-based administrator credentials for the secondary node in the Username and Password fields.

**Step 6**
Click **Next**.

Primary PAN tries to establish TLS communication (for the first time) with the node being registered.

- If the node uses a certificate that is trusted, you can proceed to step 7.

- If the node uses a self-signed certificate that is not trusted, a certificate warning message is displayed. The certificate warning message displays details about the certificate (such as, Issued-to, Issued-by, Serial number, and so on), which can be verified against the actual certificate on the node. You can select the **Import Certificate and Proceed** option to trust this certificate and proceed with registration. Cisco ISE imports the default self-signed certificate of that node to the trusted certificate store of Primary PAN. If you do not want to use the default self-signed certificate, click **Cancel Registration** and manually import the relevant certificate chain of that node to the trusted certificate store of Primary PAN. When you import the secondary node's certificate in to the trusted certificate store, check the **Trust for Authentication within ISE** check box for the PAN to validate the secondary node's certificate.

- If the node uses a CA signed certificate, an error message is displayed that the registration cannot proceed until certificate trust is set up.

**Step 7**
Select the personas and services to be enabled on the node, and then click **Save**.

When a node is registered, an alarm (which confirms that a node has been added to the deployment) will be generated on the Primary PAN. You can view this alarm on the Alarms page. After the registered node is synchronized and restarted, you can log in to the secondary node GUI using the same credentials used on Primary PAN.

What to do next

- For time-sensitive tasks such as guest user access and authorization, logging, and so on, ensure that the system time on your nodes is synchronized.

- If you registered a Secondary PAN, and will be using the internal Cisco ISE CA service, you must back up the Cisco ISE CA certificates and keys from the Primary PAN and restore them on the Secondary PAN.
**Administration Node**

A Cisco ISE node with the Administration persona allows you to perform all administrative operations on Cisco ISE. It handles all system-related configurations that are related to functionality such as authentication, authorization, auditing, and so on. In a distributed environment, you can have a maximum of two nodes running the administration persona. The administration persona can take on any one of the following roles: Standalone, Primary, or Secondary.

**High Availability for the Administrative Node**

In a high availability configuration, the Primary Administration Node (PAN) is in the active state. The Secondary PAN (backup PAN) is in the standby state, which means it receives all configuration updates from the Primary PAN, but is not active in the ISE network.

Cisco ISE supports manual and automatic failover. With automatic failover, when the Primary PAN goes down, an automatic promotion of the Secondary PAN is initiated. Automatic failover requires a non-administration secondary node, which is called a health check node. The health check node checks the health of Primary PAN. If the health detects that the Primary PAN is down or unreachable, the health check node initiates the promotion of the Secondary PAN to take over the primary role.

To deploy the auto-failover feature, you must have at least three nodes, where two of the nodes assume the Administration persona, and one node acts as the health check node. A health check node is a non-administration node and can be a Policy Service, Monitoring, or pxGrid node, or a combination of these. If the PANs are in different data centers, you must have a health check node for each PAN.

The following table lists the features that are affected when the Primary PAN goes down and the Secondary PAN is yet to take over.

<table>
<thead>
<tr>
<th>Features</th>
<th>Available When Primary PAN is Down (Yes/No)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing internal user RADIUS authentication</td>
<td>Yes</td>
</tr>
<tr>
<td>Existing or New AD user RADIUS authentication</td>
<td>Yes</td>
</tr>
<tr>
<td>Existing endpoint with no profile change</td>
<td>Yes</td>
</tr>
<tr>
<td>Existing endpoint with profile change</td>
<td>No</td>
</tr>
<tr>
<td>New endpoint learned through profiling.</td>
<td>No</td>
</tr>
<tr>
<td>Existing guest – LWA</td>
<td>Yes</td>
</tr>
<tr>
<td>Existing guest – CWA</td>
<td>Yes (apart from flows enabled for device registration, such as Hotspot, BYOD, and CWA with automatic device registration)</td>
</tr>
<tr>
<td>Guest change password</td>
<td>No</td>
</tr>
<tr>
<td>Guest – AUP</td>
<td>No</td>
</tr>
<tr>
<td>Guest – Max Failed Login Enforcement</td>
<td>No</td>
</tr>
<tr>
<td>New Guest (Sponsored or Self-registered)</td>
<td>No</td>
</tr>
</tbody>
</table>
To support certificate provisioning with the internal certificate authority, you must import the root certificate of the original Primary PAN and its key into the new primary node, after promotion. Certificate provisioning does not work after auto-failover for PSN nodes that are added after the promotion of the secondary node to Primary PAN.

### High-Availability Health Check Nodes

The health check node for Primary PAN is called the active health check node. The health check node for Secondary PAN is called the passive health check node. The active health check node is responsible for checking status of Primary PAN, and managing the automatic failover of Administration nodes. We recommended using two non-administration ISE nodes as health check nodes, one for the Primary and one for the Secondary PAN. IF you use only one health check node, and that node goes down, automatic failover will not happen.

When both PANs are in the same data center, you can use a single non-administration ISE node as the health check node for both the Primary PAN and the Secondary PAN. When a single health check node checks the health of both the Primary PAN and the Secondary PAN, it assumes both the active and passive roles.

A health check node is a non-administration node, which means it can be a Policy Service, Monitoring, or pxGrid node, or a combination of those. We recommend that you designate PSN nodes in the same data center as the Administration nodes as health check nodes. However, in a small or a centralized deployment, where the two Administration nodes are not in the same location (LAN or data center), any node (PSN/pxGrid/MnT) not having the Administration persona can be used as health check node.

If you chose not to enable automatic failover, and rely on manually promoting the secondary node when the primary PAN fails, then you do not need any check nodes.

### Health Check Node for the Secondary PAN

The health check node for the Secondary PAN is a passive monitor. It does not take any action until the Secondary PAN has been promoted as the Primary PAN. When the Secondary PAN takes over the primary role, its associated health check node takes the active role for managing automatic failover of Administration nodes. The health check node of the previous Primary PAN becomes the health check node for the Secondary PAN now and would monitor it passively.

### Disabling and Restarting Health Check

When a node is removed from the health check role or auto-failover configuration is disabled, the health check service is stopped on that node. When the auto-failover configuration is enabled on the designated high-availability health check node, the node starts checking health of Administration nodes again. Designating

---

<table>
<thead>
<tr>
<th>Features</th>
<th>Available When Primary PAN is Down (Yes/No)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Posture</td>
<td>Yes</td>
</tr>
<tr>
<td>BYOD with Internal CA</td>
<td>No</td>
</tr>
<tr>
<td>Existing Registered Devices</td>
<td>Yes</td>
</tr>
<tr>
<td>MDM On-boarding</td>
<td>No</td>
</tr>
<tr>
<td>pxGrid Service</td>
<td>No</td>
</tr>
</tbody>
</table>
or removing the high-availability health check role on a node does not involve any application restart on that node; only the health check activities are started or stopped.

If the high-availability health check node is restarted, it ignores the previous downtimes of Primary PAN and starts checking the health status afresh.

Health Check Nodes

The active health check node checks the health status of the Primary PAN at a configured polling interval. It sends a request to the Primary PAN, and if the response that it receives matches the configuration, then the health check node considers the Primary PAN to be in good health. Otherwise, the health check node considers the Primary PAN to be in bad health. If the health of the Primary PAN is bad continuously for more than the configured failover period, then the health check node initiates failover to the Secondary PAN.

If at any time during the health check, health status is found to be good after being reported as bad previously within the failover period, then the health check node marks the Primary PAN status as good, and resets the health check cycle.

Response from health check of the Primary PAN is validated against the configuration values available on its health check node. If the response does not match it would raise an alarm. However, a promotion request will be made to the Secondary PAN.

Changing Health Nodes

You can change the ISE node that you are using for a health check, but there are some things to consider.

For example, assume that the health check node (H1) goes out-of-sync and some other node (H2) is made the health check node of the Primary PAN. In such a case, once the Primary PAN goes down, there is no way for N1 to know that there is another node (H2) checking the same Primary PAN. Later, if H2 goes down or out of network, an actual failover is required. The Secondary PAN, however, retains the right to reject the promotion request. So, once the Secondary PAN has been promoted to the primary role, a promotion request from H2 is rejected with an error. Even if a health check node for the Primary PAN is out of sync, it continues to check the health of Primary PAN.

Automatic Failover to the Secondary PAN

You can configure ISE to automatically promote the secondary PAN when the primary PAN becomes unavailable. The configuration is done on the primary administrative node (Primary PAN) on the Administration > System > Deployment page. The failover period is defined as the number of times configured in Number of Failure Polls Before Failover times the number of seconds configured in Polling Interval. With the default configuration, that time is 10 minutes. Promotion of the secondary PAN to primary takes another 10 minutes. So by default, the total time from primary PAN failure to secondary PAN working is 20 minutes.

When the Secondary PAN receives the failover call, it carries out the following validations before proceeding with the actual failover:

- The Primary PAN is not available in network.
- The failover request came from a valid health check node.
- The failover request is for this PAN.

If all the validations pass, the Secondary PAN promotes itself to the primary role.
The following are some sample (but not limited to) scenarios where automatic failover of the Secondary PAN would be attempted.

- Health of Primary PAN is consistently not good for the 'Number of failure polls before failover' value during the polling period.
- Cisco ISE services on the Primary PAN are manually stopped, and remain stopped for the failover period.
- The primary PAN is shut down using soft halt or reboot option, and remains shut down for the configured failover period.
- The primary PAN goes down abruptly (power down), and remains down for the failover period.
- The network interface of Primary PAN is down (network port shut or network service down), or it is not reachable by the health check node for any other reason, and remains down for the configured failover period.

**Health Check Node Restarts**

If the high-availability health check node is restarted, it ignores the previous downtimes of Primary PAN and starts checking the health status afresh.

**Sample Scenarios when Automatic Failover is Avoided**

The following are some sample scenarios that depict cases where automatic failover by the health check node would be avoided or promotion request to the secondary node would be rejected.

- Node receiving the promotion request is not the secondary node.
- Promotion request does not have the correct Primary PAN information.
- Promotion request is received from an incorrect health check node.
- Promotion request is received but the Primary PAN is up and in good health.
- Node receiving the promotion request goes out-of-sync.

**Functionalities Affected by the PAN Auto-Failover Feature**

The following table lists the functionalities that are blocked or require additional configuration changes if PAN auto-failover configuration is enabled in your deployment.

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Affect Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations that are Blocked</td>
<td></td>
</tr>
</tbody>
</table>
## Functionalities Affected by the PAN Auto-Failover Feature

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Affect Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade</td>
<td>Upgrade via the CLI is blocked. The PAN auto-failover feature will be available for configuration after you upgrade from a previous version of Cisco ISE to release 1.4. By default, this feature is disabled. To deploy the auto-failover feature, you must have at least three nodes, where two of the nodes assume the Administration persona, and one node acts as the health check node. A health check node is a non-administration node and can be a Policy Service, Monitoring, or pxGrid node, or a combination of these. If the PANs are in different data centers, you must have a health check node for each PAN.</td>
</tr>
<tr>
<td>Restore of Backup</td>
<td>Restore via the CLI and user interface will be blocked. If PAN auto-failover configuration was enabled prior to restore, you must reconfigure it after a successful restore.</td>
</tr>
</tbody>
</table>
| Change Node Persona                | Change of the following node personas via the user interface will be blocked:  
  - Admin persona in both the Administration nodes.  
  - Persona of the PAN.  
  - Deregistration of health check node after enabling the PAN auto-failover feature. |
| Other CLI Operations               | The following admin operations via the CLI will be blocked:  
  - Patch Installation and Roll back  
  - DNS Server change  
  - IP address change of eth1, eth2, and eth3 interfaces  
  - Host alias change of eth1, eth2, and eth3 interfaces  
  - Timezone change |
### Configure Primary PAN for Automatic Failover

**Before you begin**

To deploy the auto-failover feature, you must have at least three nodes, where two of the nodes assume the Administration persona, and one node acts as the health check node. A health check node is a non-administration node and can be a Policy Service, Monitoring, or pxGrid node, or a combination of these. If the PANs are in different data centers, you must have a health check node for each PAN.

#### Step 1
Log in to the user interface of the Primary PAN.

#### Step 2
Choose **Administration > System > Deployment > PAN Failover**.

#### Step 3
Check the **Enable PAN Auto Failover** check box, to enable automatic failover of the Primary PAN.

You can only promote a Secondary PAN to become the Primary PAN. Cisco ISE nodes that assume only the Policy Service, Monitoring, or pxGrid persona, or a combination of these, cannot be promoted to become the Primary PAN.

#### Step 4
Select the health check node for Primary PAN from the **Primary Health Check Node** drop down list containing all the available secondary nodes.

It is recommended to have this node in the same location or data center as the Primary PAN.
Step 5  Select the health check node for Secondary PAN, from the **Secondary Health Check Node** drop down list containing all the available secondary nodes.

It is recommended to have this node in the same location or data center as the Secondary PAN.

Step 6  Provide the **Polling Interval** time after which the Administration node status will be checked. The valid range is from 30 to 300 seconds.

Step 7  Provide the count for **Number of Failure Polls before Failover**.

The failover will occur if the status of the Administration node is not good for the specified number of failure polls. The valid range is from 2 to 60 counts.

Step 8  Click **Save**.

---

**What to do next**

After the promotion of Secondary PAN to the Primary PAN, do the following:

- Manually sync the old Primary PAN to bring it back into the deployment.
- Manually sync any other secondary node that is out-of-sync, to bring it back into the deployment.

---

**Manually Promote Secondary PAN To Primary**

If the Primary PAN fails and you have not configured PAN auto-failover, you must manually promote the Secondary PAN to become the new Primary PAN.

**Before you begin**

Ensure that you have a second Cisco ISE node configured with the Administration persona to promote as your Primary PAN.

---

**Step 1**  Log in to the user interface of the Secondary PAN.

**Step 2**  Choose **Administration > System > Deployment**.

**Step 3**  In the Edit Node page, click **Promote to Primary**.

You can only promote a Secondary PAN to become the Primary PAN. Cisco ISE nodes that assume only the Policy Service or Monitoring persona, or both, cannot be promoted to become the Primary PAN.

**Step 4**  Click **Save**.

---

**What to do next**

If the node that was originally the Primary PAN comes back up, it will be demoted automatically and become the Secondary PAN. You must perform a manual synchronization on this node (that was originally the Primary PAN) to bring it back into the deployment.

In the Edit Node page of a secondary node, you cannot modify the personas or services because the options are disabled. You have to log in to the Admin portal to make changes.
Restoring Service to the Primary PAN

Cisco ISE does not support automatic fallback to original Primary PAN. After the automatic failover to the Secondary PAN is initiated, if you bring the original Primary PAN back into the network, you should configure it as the secondary PAN.

Policy Service Node

A Cisco ISE node with the Policy Service persona provides network access, posture, guest access, client provisioning, and profiling services. This persona evaluates the policies and makes all the decisions. You can have more than one node assume this persona. Typically, there would be more than one Policy Service node in a distributed deployment. All Policy Service nodes that reside in the same high-speed Local Area Network (LAN) or behind a load balancer can be grouped together to form a node group. If one of the nodes in a node group fails, the other nodes detect the failure and reset any URL-redirected sessions.

At least one node in your distributed setup should assume the Policy Service persona.

High Availability in Policy Service Nodes

To detect node failure and to reset all URL-redirected sessions on the failed node, two or more Policy Service nodes can be placed in the same node group. When a node that belongs to a node group fails, another node in the same node group issues a Change of Authorization (CoA) for all URL-redirected sessions on the failed node.

All the nodes within the same node group should be configured on the network access device (NAD) as RADIUS clients and authorized for CoA, because any one of them can issue a CoA request for the sessions that are established through any node in the node group. If you are not using a load balancer, the nodes in a node group should be the same as, or a subset of, the RADIUS servers and clients configured on the NAD. These nodes would also be configured as RADIUS servers.

While a single NAD can be configured with many ISE nodes as RADIUS servers and dynamic-authorization clients, it is not necessary for all the nodes to be in the same node group.

The members of a node group should be connected to each other using high-speed LAN connection such as Gigabit Ethernet. The node group members need not be L2 adjacent, but L2 adjacency is highly recommended to ensure sufficient bandwidth and reachability. See Create a Policy Service Node Group, on page 70 section for more details.

Load Balancer To Distribute Requests Evenly Among PSNs

When you have multiple Policy Service nodes in the deployment, you can use a load balancer to distribute the requests evenly. The load balancer distributes the requests to the functional nodes behind it. Refer to the Cisco and F5 Deployment Guide: ISE Load Balancing using BIG-IP for information on and best practices about deploying PSNs behind a load balancer.

Session Failover in Policy Service Nodes

When a Policy Service node that has active URL-redirected sessions fails, the endpoints are stuck in an intermediate state. Even if the redirect endpoint detects that the Policy Service node that it has been communicating with has failed, it cannot re-initiate authorization.
If the Policy Service nodes are part of a node group, the nodes within a node group exchange heartbeat messages to detect node failures. If a node fails, one of its peers from the node group learns about the active URL-redirected sessions on the failed node and issues a CoA to disconnect those sessions.

As a result, the sessions are handled by another Policy Service node that is available in the same node group. The session failover does not automatically move the sessions over from a Policy Service node that has gone down to one that is available, but issues a CoA to achieve that.

The Policy Service nodes in a distributed deployment do not share their Machine Access Restriction (MAR) cache with each other. If you have enabled the MAR feature in Cisco ISE and the client machine is authenticated by a Policy Service node that fails, then another Policy Service node in the deployment handles the user authentication. However, the user authentication fails because the second Policy Service node does not have the host authentication information in its MAR cache.

Number of Nodes in a Policy Service Node Group

The number of nodes that you can have in a node group depends on your deployment requirements. Node groups ensure that node failures are detected and that a peer issues a CoA for sessions that are authorized, but not yet postured. The size of the node group does not have to be very large.

If the size of the node group increases, the number of messages and heartbeats that are exchanged between nodes increases significantly. As a result, traffic also increases. Having fewer nodes in a node group helps reduce the traffic and at the same time provides sufficient redundancy to detect Policy Service node failures.

There is no hard limit on the number of Policy Service nodes that you can have in a node group cluster.

Monitoring Node

A Cisco ISE node with the Monitoring persona functions as the log collector and stores log messages from all the administration and Policy Service nodes in your network. This persona provides advanced monitoring and troubleshooting tools that you can use to effectively manage your network and resources. A node with this persona aggregates and correlates the data that it collects to provide you with meaningful information in the form of reports.

Cisco ISE allows you to have a maximum of two nodes with this persona that can take on primary or secondary roles for high availability. Both the primary and secondary Monitoring nodes collect log messages. In case the primary Monitoring node goes down, the secondary Monitoring node automatically becomes the primary Monitoring node.

At least one node in your distributed setup should assume the Monitoring persona. We recommend that you not have the Monitoring and Policy Service personas enabled on the same Cisco ISE node. We recommend that the node be dedicated solely to monitoring for optimum performance.

You can access the Monitoring menu from the PAN in your deployment.

Automatic Failover in Monitoring Nodes

The term automatic failover is used because high availability is not supported on Monitoring nodes in the true sense. For Monitoring nodes, operation audit data is duplicated by the Policy Service node(s), which then sends copies to both the primary and secondary Monitoring nodes.
**Note**
Monitoring is served from the primary (active) Monitoring node. Monitoring data is only served from the secondary (standby) Monitoring node when the active node is down. The secondary monitoring node is read-only.

**Automatic Failover Process**
When a primary Monitoring node goes down, the secondary Monitoring node takes over all monitoring and troubleshooting information. The secondary node provides read-only capabilities.

To convert the existing secondary node to an active primary node, the administrator must first manually promote the secondary node to a primary role. If the primary node comes back up after the secondary node has been promoted, it assumes the secondary role. If the secondary node was not promoted, the primary Monitoring node will resume its role after it comes back up.

**Caution**
When the primary node comes back up after a failover, obtain a backup and restore the data to update the primary node.

**Guidelines for Setting Up an Active-Standby Pair of Monitoring Nodes**
You can specify two Monitoring nodes on an ISE network and create an active-standby pair. When you register a secondary Monitoring node, we recommend that you back up the primary Monitoring node and then restore the data to the new secondary Monitoring node. This ensures that the history of the primary Monitoring node is in sync with the new secondary node as new changes are replicated. Once the active-standby pair is defined, the following rules apply:

- All changes must be made on the primary Monitoring node. The secondary node is read-only.
- Changes made to the primary node are automatically replicated on the secondary node.
- Both the primary and secondary nodes are listed as log collectors to which all other nodes send logs.
- The Cisco ISE dashboard is the main entry point for monitoring and troubleshooting. Monitoring information is displayed on the dashboard from the PAN. If the primary node goes down, the information is served from the secondary node.
- Backing up and purging monitoring data is not part of a standard Cisco ISE node backup process. You must configure repositories for backup and data purging on both the primary and secondary Monitoring nodes, and use the same repositories for each.

**Monitoring Node Failover Scenarios**
The following scenarios apply to the active-standby or single node configurations corresponding to the monitoring nodes:

- In an active-standby configuration of the monitoring nodes, the Primary Administration Node (PAN) always points to the active monitoring node to collect the monitoring data. After the active monitoring node fails, the PAN points to the standby monitoring node. The failover from the active monitoring node to the standby monitoring node happens after it is down for more than 5 minutes.
However, after the active node fails, the standby node does not become the active node. In case the active node comes up, the Administration node starts collecting the monitoring data again from the resumed active node.

- During the time that the active monitoring node is down, if you want to promote the standby monitoring node to active status, you must de-register the existing active monitoring node. When you de-register the existing active monitoring node, the standby node becomes the active monitoring node and the PAN automatically starts pointing to the newly promoted active node.

- In an active-standby pair, if you choose to de-register the standby monitoring node from the deployment or if the standby monitoring node goes down, the existing active monitoring node still retains the active node status. The PAN points to the existing active node for data collection.

- If there is only one monitoring node in the ISE deployment, then that node acts as the active monitoring node that provides monitoring data to the PAN. However, when you register a new monitoring node and make it the active node in the deployment, the existing active monitoring node automatically becomes the standby node. The PAN begins to point to the newly registered active monitoring node for collecting monitoring data.

pxGrid Node

You can use Cisco pxGrid to share the context-sensitive information from Cisco ISE session directory with other network systems such as ISE Eco system partner systems and other Cisco platforms. The pxGrid framework can also be used to exchange policy and configuration data between nodes like sharing tags and policy objects between Cisco ISE and third party vendors, and for other information exchanges. pxGrid also allows 3rd party systems to invoke adaptive network control actions (EPS) to quarantine users/devices in response to a network or security event. The TrustSec information like tag definition, value, and description can be passed from Cisco ISE via TrustSec topic to other networks. The endpoint profiles with Fully Qualified Names (FQNs) can be passed from Cisco ISE to other networks through a endpoint profile meta topic. Cisco pxGrid also supports bulk download of tags and endpoint profiles.

You can publish and subscribe to SXP bindings (IP-SGT mappings) through pxGrid. For more information about SXP bindings, see Security Group Tag Exchange Protocol, on page 847.

In a high-availability configuration, Cisco pxGrid servers replicate information between the nodes through the PAN. When the PAN goes down, pxGrid server stops handling the client registration and subscription. You need to manually promote the PAN for the pxGrid server to become active. You can check the pxGrid Services page (Administration > pxGrid Services) to verify whether a pxGrid node is currently in active or standby state.

For XMPP (Extensible Messaging and Presence Protocol) clients, pxGrid nodes work in Active/Standby high availability mode which means that the pxGrid Service is in "running" state on the active node and in "disabled" state on the standby node.

After the automatic failover to the secondary pxGrid node is initiated, if the original primary pxGrid node is brought back into the network, the original primary pxGrid node will continue to have the secondary role and will not be promoted back to the primary role unless the current primary node goes down.

---

Note

At times, the original primary pxGrid node might be automatically promoted back to the primary role.
In a high availability deployment, when the primary pxGrid node goes down, it might take around 3 to 5 minutes to switchover to the secondary pxGrid node. It is recommended that the client waits for the switchover to complete, before clearing the cache data in case of primary pxGrid node failure.

The following logs are available for pxGrid node:

- `pxgrid.log`—State change notifications.
- `pxgrid-cm.log`—Updates on publisher/subscriber and data exchange activity between client and server.
- `pxgrid-controller.log`—Displays the details of client capabilities, groups, and client authorization.
- `pxgrid-jabberd.log`—All logs related to system state and authentication.
- `pxgrid-pubsub.log`—Information related to publisher and subscriber events.

---

**Note**

If pxGrid service is disabled on a node, port 5222 will be down, but port 8910 (used by Web Clients) will be functional and will continue to respond to the requests.

---

**Note**

You can enable pxGrid with Base license, but you must have a Plus license to enable pxGrid persona. In addition, certain extended pxGrid services may be available in your Base installation if you have recently installed an upgrade license for.

---

**Note**

pxGrid should be defined in order to work with the Passive ID Work Center. For more information, see Passive ID Work Center, on page 359.

---

**pxGrid Client and Capability Management**

Clients connected to Cisco ISE need to register to use the pxGrid services. pxGrid clients should adopt the pxGrid Client Library available from Cisco through the pxGrid SDK to become the clients. Cisco pxGrid clients need an approved account to participate in pxGrid services. Cisco ISE supports both auto and manual approvals. A client can log in to pxGrid using a unique name and certificate-based mutual authentication. Similar to the AAA setting on a switch, clients can connect to either a configured pxGrid server host-name or an IP Address.

Capabilities are information topics or channels created on pxGrid for clients to publish and subscribe. In Cisco ISE, only capabilities such as Identity, adaptive network control, and SGA are supported. When a client creates a new capability, it appears in Administration > pxGrid Services > View by Capabilities. You can enable or disable capabilities individually. Capability information is available from the publisher through publish, directed query, or bulk download query.

---

**Note**

Users that are assigned to EPS user group can perform actions in Session group, because pxGrid Session group is part of EPS group. If a user is assigned to EPS group, the user will be able to subscribe to Session group on pxGrid client.
Enable pxGrid Clients

Before you begin

• Enable the pxGrid persona on at least one node to view the requests from the Cisco pxGrid clients.
• Enable Passive Identity Services. Choose Administration > Deployment, checkmark the desired node, click Edit and from the settings screen, checkmark Enable Passive Identity Service.

Step 1  Choose Administration > pxGrid Services.
Step 2  Check the checkbox next to the client and click Approve.
Step 3  Click Refresh to view the latest status.

Enable pxGrid Capabilities

Before you begin

• Enable the pxGrid persona on at least one node to view the requests from the Cisco pxGrid clients.
• Enable a pxGrid client.

Step 1  Choose Administration > pxGrid Services.
Step 2  Click View by Capabilities at the top-right.
Step 3  Select the capability you want to enable and click Enable.
Step 4  Click Refresh to view the latest status.

Cisco pxGrid Live Logs

The Live Logs page displays all the pxGrid management events. Event info includes the client and capability names along with the event type and timestamp.

Navigate to Administration > pxGrid Services > Live Log to view the list of events. You can also clear the logs and resynchronize or refresh the list.

Configure pxGrid Settings

Before you begin

To perform the following task, you must be a Super Admin or System Admin.
Step 1 Choose Administration > pxGrid Services > Settings.
Step 2 Select the following options based on your requirements:

- Automatically Approve New Accounts—Check this check box to automatically approve the connection requests from new pxGrid clients.

- Allow Password Based Account Creation—Check this check box to enable username/password based authentication for pxGrid clients. If this option is enabled, the pxGrid clients cannot be automatically approved.

A pxGrid client can register itself with the pxGrid controller by sending the username via REST API. The pxGrid controller generates a password for the pxGrid client during client registration. The administrator can approve or deny the connection request.

Step 3 Click Save.

You can use the Test option on the pxGrid Settings page to run a health check on the pxGrid node. You can view the details in the pxgrid/pxgrid-test.log file.

**Generate pxGrid Certificate**

**Before you begin**

- To perform the following task, you must be a Super Admin or System Admin.

- pxGrid certificate must be generated from the Primary PAN.

- If the pxGrid certificate uses the subject alternative name (SAN) extension, be sure to include the FQDN of the subject identity as a DNS name entry.

Step 1 Choose Administration > pxGrid Services > Certificates.
Step 2 Select one of the following options from the I want to drop-down list:

- Generate a single certificate without a certificate signing request—You must enter the Common Name (CN) if you select this option.

- Generate a single certificate with a certificate signing request—You must enter the Certificate Signing Request details if you select this option.

- Generate bulk certificates—You can upload a CSV file that contains the required details.

- Download root certificate chain—You can download the root certificates and add them to the trusted certificate store. You must specify the host name and the certificate download format.

You can download the certificate template from the Certificate Template link and edit the template based on your requirements.

Step 3 (Required if you choose to Generate a single certificate (without a certificate signing request) option) Enter the FQDN of the pxGrid client.

Step 4 (optional) You can enter a description for this certificate.
Step 5 Specify the Subject Alternative Name (SAN). You can add multiple SANs. The following options are available:

- IP address—Enter the IP address of the pxGrid client to be associated with the certificate.
- FQDN—Enter the fully qualified domain name of the pxGrid client.

**Note** This field is not displayed if you have selected the Generate Bulk Certificate option.

Step 6 Select one of the following options from the **Certificate Download Format** drop-down list:

- Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)—The root certificate, the intermediate CA certificates, and the end entity certificate are represented in the PEM format. PEM formatted certificate are BASE64-encoded ASCII files. Each certificate starts with the "--------BEGIN CERTIFICATE-----" tag and ends with the "--------END CERTIFICATE-----" tag. The end entity’s private key is stored using PKCS* PEM. It starts with the "-----BEGIN ENCRYPTED PRIVATE KEY-----" tag and ends with the "-----END ENCRYPTED PRIVATE KEY-----" tag.
- PKCS12 format (including certificate chain; one file for both the certificate chain and key)—A binary format to store the root CA certificate, the intermediate CA certificate, and the end entity’s certificate and private key in one encrypted file.

Step 7 Enter a certificate password.

Step 8 Click **Create**.

The certificate that you created is visible in ISE under *Administration* > *System* > *Certificates* > *Certificate Authority* > *Issued Certificates*, and downloaded to your browser's downloads directory.

### View Nodes in a Deployment

In the Deployment Nodes page, you can view all the Cisco ISE nodes, primary and secondary, that are part of your deployment.

**Step 1** Log in to the primary Cisco ISE Admin portal.

**Step 2** Choose *Administration* > *System* > *Deployment*.

**Step 3** Click **Deployment** from the navigation pane on the left.

All the Cisco ISE nodes that are part of your deployment are listed.

### Synchronize Primary and Secondary Cisco ISE Nodes

You can make configuration changes to Cisco ISE only through the Primary PAN. The configuration changes get replicated to all the secondary nodes. If, for some reason, this replication does not occur properly, you can manually synchronize the Secondary PAN with the Primary PAN.
Before you begin

You must click the Syncup button to force a full replication if the Sync Status is set to Out of Sync or if the Replication Status is Failed or Disabled.

---

### Step 1
Log in to the Primary PAN.

### Step 2
Choose Administration > System > Deployment.

### Step 3
Check the check box next to the node that you want to synchronize with the Primary PAN, and click Syncup to force a full database replication.

---

### Change Node Personas and Services

You can edit the Cisco ISE node configuration to change the personas and services that run on the node.

#### Before you begin

- When you enable or disable any of the services that run on a Policy Service node or make any changes to a Policy Service node, you will be restarting the application server processes on which these services run. Expect a delay while these services restart.

- Due to this delay in restart of services, auto-failover if enabled in your deployment, might get initiated. To avoid this, make sure that the auto-failover configuration is turned off.

---

### Step 1
Log in to the Primary PAN.

### Step 2
Choose Administration > System > Deployment.

### Step 3
Check the check box next to the node whose personas or services you want to change, and then click Edit.

### Step 4
Choose the personas and services that you want.

### Step 5
Click Save.

### Step 6
Verify receipt of an alarm on your Primary PAN to confirm the persona or service change. If the persona or service change is not saved successfully, an alarm is not generated.

---

### Effects of Modifying Nodes in Cisco ISE

When you make any of the following changes to a node in a Cisco ISE ISE, that node restarts, which causes a delay:

- Register a node (Standalone to Secondary)
- Deregister a node (Secondary to Standalone)
- Change a primary node to Standalone (if no other nodes are registered with it; Primary to Standalone)
- Promote an Administration node (Secondary to Primary)
• Change the personas (when you assign or remove the Policy Service or Monitoring persona from a node)
• Modify the services in the Policy Service node (enable or disable the session and profiler services)
• Restore a backup on the primary and a sync up operation is triggered to replicate data from primary to secondary nodes

Create a Policy Service Node Group

When two or more Policy Service nodes (PSNs) are connected to the same high-speed Local Area Network (LAN), we recommend that you place them in the same node group. This design optimizes the replication of endpoint profiling data by retaining less significant attributes local to the group and reducing the information that is replicated to the remote nodes in the network. Node group members also check on the availability of peer group members. If the group detects that a member has failed, it attempts to reset and recover all URL-redirected sessions on the failed node.

Note

Before you can add PSNs as members to a node group, you must create the node group first. You can create, edit, and delete Policy Service node groups from the Deployment pages of the Admin portal.

Before you begin

Node group members can communicate over TCP/7800.

Step 1
Choose Administration > System > Deployment.

Step 2
Click the action icon, and then click Create Node Group.

Step 3
Enter a unique name for your node group.

Step 4
(Optional) Enter a description for your node group.

Step 5
Check the Enable MAR Cache Distribution check box and fill in the other options. Ensure that the MAR is enabled in the Active Directory page before enabling this option.

Step 6
Click Submit to save the node group.

After you save the node group, it should appear in the navigation pane on the left. If you do not see the node group in the left pane, it may be hidden. Click the Expand button on the navigation pane to view the hidden objects.

What to do next

Add a node to a node group. Edit the node by choosing the node group from the Member of Node Group drop-down list.
Deploy pxGrid Node

You can enable Cisco pxGrid persona both on a standalone node and distributed deployment node.

Before you begin

- You can enable pxGrid with Base license, but you must have a Plus license to enable pxGrid persona.
- Cisco pxGrid services running on a Cisco ISE SNS 3415/3495 Appliance or in VMWare.
- All nodes are configured to use the CA certificate for pxGrid usage. If default certificate is used for pxGrid before upgrade, it will be replaced by the internal CA certificate after upgrade.
- If you are using a distributed deployment or upgrading from Cisco ISE 1.2, then you need to enable the pxGrid Usage option for the certificates. To enable the pxGrid Usage option, go to Administration > Certificates > System Certificates. Choose the certificate being used in the deployment and click Edit. Check the pxGrid: use certificate for the pxGrid Controller checkbox.

Step 1    Choose Administration > System > Deployment.
Step 2    In the Deployment Nodes page, check the check box next to the node to which you want to enable the pxGrid services, and click Edit.
Step 3    Click the General Settings tab and check the pxGrid checkbox.
Step 4    Click Save.

When you upgrade from the previous version, the Save option might be disabled. This happens when the browser cache refers to the old files from the previous version of Cisco ISE. Clear the browser cache to enable the Save option.

Configure Monitoring Nodes for Automatic Failover

If you have two Monitoring nodes in a deployment, you can configure a primary-secondary pair for automatic failover to avoid downtime in the Cisco ISE Monitoring service. A primary-secondary pair ensures that a secondary Monitoring node automatically provides monitoring should the primary node fail.

Before you begin

- Before you can configure Monitoring nodes for automatic failover, they must be registered as Cisco ISE nodes.
- Configure monitoring roles and services on both nodes and name them for their primary and secondary roles, as appropriate.
- Configure repositories for backup and data purging on both the primary and secondary Monitoring nodes. For the backup and purging features to work properly, use the same repositories for both the nodes. Purging takes place on both the primary and secondary nodes of a redundant pair. For example, if the primary Monitoring node uses two repositories for backup and purging, you must specify the same repositories for the secondary node.
- Configure a data repository for a Monitoring node using the repository command in the system CLI.
For scheduled backup and purge to work properly on the nodes of a Monitoring redundant pair, configure the same repository, or repositories, on both the primary and secondary nodes using the CLI. The repositories are not automatically synced between the two nodes.

From the Cisco ISE dashboard, verify that the Monitoring nodes are ready. The System Summary dashlet shows the Monitoring nodes with a green check mark to the left when their services are ready.

**Step 1** Choose **Administration** > **System** > **Deployment**.

**Step 2** In the Deployment Nodes page, check the check box next to the Monitoring node that you want to specify as active, and click **Edit**.

**Step 3** Click the **General Settings** tab and choose **Primary** from the **Role** drop-down list. When you choose a Monitoring node as primary, the other Monitoring node automatically becomes secondary. In the case of a standalone deployment, primary and secondary role configuration is disabled.

**Step 4** Click **Save**. The active and standby nodes restart.

---

## Remove a Node from Deployment

To remove a node from a deployment, you must deregister it. The deregistered node becomes a standalone Cisco ISE node.

It retains the last configuration that it received from the Primary PAN and assumes the default personas of a standalone node that are Administration, Policy Service, and Monitoring. If you deregister a Monitoring node, this node will no longer be a syslog target.

When a Primary PSN is deregistered, the endpoint data is lost. If you want the PSN to retain the endpoint data after it becomes a standalone node, you can do one of the following:

- Obtain a backup from the Primary PAN and when the PSN becomes a standalone node, restore this data backup on it.

- Change the persona of the PSN to Administration (Secondary PAN), synchronize the data from the deployment page of the Admin portal, and then deregister the node. This node will now have all the data. You can then add a Secondary PAN to the existing deployment.

You can view these changes from the Deployment page of the Primary PAN. However, expect a delay of 5 minutes for the changes to take effect and appear on the Deployment page.

**Before you begin**

Before you remove any secondary node from a deployment, perform a backup of Cisco ISE configuration, which you can then restore later on, if needed.

**Step 1** Choose **Administration** > **System** > **Deployment**.
Step 2: Check the check box next to the secondary node that you want to remove, and then click **Deregister**.

Step 3: Click **OK**.

Step 4: Verify receipt of an alarm on your Primary PAN to confirm that the secondary node is deregistered successfully. If the secondary node fails to deregister from the Primary PAN, the alarm is not generated.

---

### Change the Hostname or IP Address of a Standalone Cisco ISE Node

You can change the hostname, IP address, or domain name of standalone Cisco ISE nodes. You cannot use "localhost" as the hostname for a node.

**Before you begin**

If the Cisco ISE node is part of a distributed deployment, you must first remove it from the deployment and ensure that it is a standalone node.

**Step 1** Change the hostname or IP address of the Cisco ISE node using the `hostname`, `ip address`, or `ip domain-name` command from the Cisco ISE CLI.

**Step 2** Reset the Cisco ISE application configuration using the `application stop ise` command from the Cisco ISE CLI to restart all the services.

**Step 3** Register the Cisco ISE node to the Primary PAN if it is part of a distributed deployment.

**Note**

If you are using the hostname while registering the Cisco ISE node, the fully qualified domain name (FQDN) of the standalone node that you are going to register, for example, `abc.xyz.com` must be DNS-resolvable from the Primary PAN. Otherwise, node registration fails. You must enter the IP addresses and FQDNs of the Cisco ISE nodes that are part of your distributed deployment in the DNS server.

After you register the Cisco ISE node as a secondary node, the Primary PAN replicates the change in the IP address, hostname, or domain name to the other Cisco ISE nodes in your deployment.

---

### Replace the Cisco ISE Appliance Hardware

You should replace the Cisco ISE appliance hardware only if there is an issue with the hardware. For any software issues, you can reimage the appliance and reinstall the Cisco ISE software.

**Step 1** Re-image or re-install the Cisco ISE software on the new nodes.

**Step 2** Obtain a license with the UDI for the Primary and Secondary PANs and install it on the Primary PAN.

**Step 3** Restore the backup on the replaced Primary PAN.

The restore script will try to sync the data on the Secondary PAN, but the Secondary PAN is now a standalone node and the sync will fail. Data is set to the time the backup was taken on the Primary PAN.
Step 4  
Register the new node as a secondary server with the Primary PAN.
PART III

Setup Cisco ISE Management Access

• Administer Cisco ISE, on page 77
• Manage Administrators and Admin Access Policies, on page 99
• Cisco ISE Licenses, on page 127
• Manage Certificates, on page 137
• Control Device Administration Using TACACS+, on page 195
• Manage Network Devices, on page 209
• Manage Resources, on page 261
• Logging Mechanism, on page 267
• Backup and Restore Operations, on page 279
• Setup Adaptive Network Control, on page 299
Administer Cisco ISE

- Administrator Access to Cisco ISE, on page 77
- Specify Proxy Settings in Cisco ISE, on page 79
- Ports Used by the Admin Portal, on page 79
- Enable External RESTful Services APIs, on page 79
  - External RESTful Services SDK, on page 80
- Specify System Time and NTP Server Settings, on page 81
- Changing the System Time Zone, on page 82
- Configure SMTP Server to Support Notifications, on page 82
- Cisco ISE Deployment Upgrade, on page 83
- Cisco ISE Software Patches, on page 87
- Roll Back Software Patches, on page 88
- View Patch Install and Rollback Changes, on page 89
- FIPS Mode Support, on page 90
- Securing SSH Key Exchange Using Diffie-Hellman Algorithm, on page 94
- Configure Cisco ISE to Send Secure Syslog, on page 94
- Default Secure Syslog Collector, on page 96
- Offline Maintenance, on page 97

Administrator Access to Cisco ISE

You can connect to ISE servers in several ways. The PAN runs the Administrators portal, which requires the admin password to log in. Other ISE persona servers can be accessed by SSH or the console, where you run the CLI. This section describes the process and password options available for each connection type.

- **Admin password**: The ISE Admin user that you created during installation is configured to time out in 45 days by default. You can prevent that by turning off password time on **Administration > System > Admin Settings**. Chose the **Password Policy** tab, and uncheck **Administrative passwords expire** under **Password Lifetime**.

  If you don’t do this, and the password expires, you can reset the Admin password in the CLI. The CLI command is **application reset-passwd**. You can either connect to the console to access the CLI, or reboot the ISE image file to access the boot options menu, to reset the Admin menu.

- **CLI password**: The CLI password is specified during installation. If you have a problem logging in with to the CLI because of an invalid password, you can reset the CLI password by connecting to console and running the **password** CLI command. See the ISE CLI Reference for more information.
SSH access to the CLI: You either enable SSH access during installation, or after, using the CLI command `service sshd`. You can also force SSH connections to use a key. Note that when you do that, SSH connections to all network devices will also use that key, see SSH Key Validation, on page 840. You can force the SSH key to use the Diffie-Hellman Algorithm Securing SSH Key Exchange Using Diffie-Hellman Algorithm, on page 94. ECDSA keys are not supported for SSH keys.

The following steps describe how to log into the Administrative portal.

**Step 1**
Enter the Cisco ISE URL in the address bar of your browser (for example, https://<ise hostname or ip address>/admin/).

**Step 2**
Enter the username and case-sensitive password, that was specified and configured during the initial Cisco ISE setup.

**Step 3**
Click **Login** or press **Enter**.

If your login is unsuccessful, click the **Problem logging in?** link in the Login page and follow the instructions.

---

**Related Topics**

Administrator Login Browser Support, on page 78

---

**Administrator Login Browser Support**

The Cisco ISE Admin portal supports the following HTTPS-enabled browsers:

- Mozilla Firefox 61 and earlier versions
- Google Chrome 67 and earlier versions
- Microsoft Internet Explorer 10.x and 11.x

If you are using Internet Explorer 10.x, enable TLS 1.1 and TLS 1.2, and disable SSL 3.0 and TLS 1.0 (Internet Options > Advanced).

---

**ISE Community Resource**

ISE Pages Fail to Fully Load When Adblock Plus is Used

---

**Administrator Lockout Following Failed Login Attempts**

If you enter an incorrect password for your specified administrator user ID enough times, the Admin portal “locks you out” of the system, adds a log entry in the Server Administrator Logins report, and suspends the credentials for that administrator ID until you have an opportunity to reset the password that is associated with that administrator ID, as described in the “Performing Post-Installation Tasks” chapter of the Cisco Identity Services Engine Hardware Installation Guide. The number of failed attempts that is required to disable the administrator account is configurable according to the guidelines that are described in 'User Account Custom Attributes and Password Policies' section. After an administrator user account gets locked out, an e-mail is sent to the associated administrator user.

Disabled System administrators' status can be enabled by any Super Admin, including Active Directory users.
Specify Proxy Settings in Cisco ISE

If your existing network topology requires you to use a proxy for Cisco ISE, to access external resources (such as the remote download site where you can find client provisioning and posture-related resources), you can use the Admin portal to specify proxy properties.

The proxy settings impact the following Cisco ISE functions:
- Partner Mobile Management
- Endpoint Profiler Feed Service Update
- Endpoint Posture Update
- Endpoint Posture Agent Resources Download
- CRL (Certificate Revocation List) Download
- Guest Notifications

The Cisco ISE proxy configuration supports basic authentication for proxy servers. NT LAN Manager (NTLM) authentication is not supported.

Step 1
Choose Administration > System > Settings > Proxy.

Step 2
Enter the proxy IP address or DNS-resolvable host name and specify the port through which proxy traffic travels to and from Cisco ISE in Proxy Host server : port.

Step 3
Check Password required check box, if required.

Step 4
Enter the user name and password used to authenticate to the proxy servers in the User Name and Password fields.

Step 5
Enter the IP address or address range of hosts or domains to be bypassed in Bypass proxy for these hosts and domain.

Step 6
Click Save.

Ports Used by the Admin Portal

The Admin portal is set to use HTTP port 80 and HTTPS port 443, and you cannot change these settings. Cisco ISE also prevents you from assigning any of the end-user portals to use the same ports, which reduces the risk to the Admin portal.

Enable External RESTful Services APIs

The External RESTful Services APIs are based on HTTPS protocol and REST methodology and uses port 9060.

The External RESTful Services APIs support basic authentication. The authentication credentials are encrypted and are part of the request header.

You can use any REST client like JAVA, curl linux command, python or any other client to invoke External RESTful Services API calls.

The ISE administrator must assign special privileges to a user to perform operations using the External RESTful Services APIs. To perform operations using the External RESTful Services APIs (except for the Guest API),
the users must be assigned to one of the following Admin Groups and must be authenticated against the credentials stored in the Cisco ISE internal database (internal admin users):

- External RESTful Services Admin—Full access to all ERS APIs (GET, POST, DELETE, PUT). This user can Create, Read, Update, and Delete ERS API requests.
- External RESTful Services Operator—Read Only access (GET request only).

Note

The Super Admin user can access all ERS APIs.

The External RESTful Services APIs are not enabled by default. If you try to evoke the External RESTful Services API calls before enabling them, you will receive an error response. You must enable the Cisco ISE REST API in order for applications developed for a Cisco ISE REST API to be able to access Cisco ISE. The Cisco REST APIs uses HTTPS port 9060, which is closed by default. If the Cisco ISE REST APIs are not enabled on the Cisco ISE admin server, the client application will receive a time-out error from the server for any Guest REST API request.

---

**Step 1** Choose **Administration > Settings > ERS Settings**.

**Step 2** Choose **Enable ERS for Read/Write** for the Primary Administration Node.

**Step 3** Choose **Enable ERS for Read for All Other Nodes** if there are any secondary nodes.

External RESTful Service requests of all types are valid only for the primary ISE node. Secondary nodes have read-access (GET requests).

**Step 4** Select one of the following options:

- Use CSRF Check for Enhanced Security—If this option is enabled, the ERS client must send a GET request to fetch the Cross-Site Request Forgery (CSRF) token from Cisco ISE and include the CSRF token in the requests sent to Cisco ISE. Cisco ISE will validate the CSRF token when a request is received from the ERS client. Cisco ISE processes the request only if the token is valid. This option is not applicable for pre ISE 2.3 Clients.

- Disable CSRF for ERS Request—If this option is enabled, CSRF validation is not performed. This option can be used for pre ISE 2.3 Clients.

**Step 5** Click **Submit**.

All REST operations are audited and the logs are logged in the system logs. External RESTful Services APIs have a debug logging category, which you can enable from the debug logging page of the Cisco ISE GUI.

**Related Topics**

External RESTful Services SDK, on page 80

---

**External RESTful Services SDK**

You can use the External RESTful Services SDK to start building your own tools. You can access the External RESTful Services SDK from the following URL: https://<ISE-ADMIN-NODE>:9060/ers/sdk. External RESTful Services SDK can be accessed by the External RESTful Services Admin users only.

The SDK consists the following components:
Specify System Time and NTP Server Settings

Cisco ISE allows you to configure up to three Network Time Protocol (NTP) servers. You can use the NTP servers to maintain accurate time and synchronize time across different timezones. You can also specify whether or not Cisco ISE should use only authenticated NTP servers, and you can enter one or more authentication keys for that purpose.

Cisco recommends that you set all Cisco ISE nodes to the Coordinated Universal Time (UTC) timezone—especially if your Cisco ISE nodes are installed in a distributed deployment. This procedure ensures that the reports and logs from the various nodes in your deployment are always in sync with regard to the timestamps.

Cisco ISE also supports public-key authentication for NTP servers. NTPv4 uses symmetric-key cryptography and also provides a new Autokey scheme based on public-key cryptography. Public-key cryptography is generally considered more secure than symmetric-key cryptography because the security is based on a private value, which is generated by each server and never revealed. With Autokey, all key distribution and management functions involve only public values, which considerably simplifies key distribution and storage.

You can configure Autokey for NTP server from the Cisco ISE CLI in Configuration Mode. We recommend that you use the IFF (identify Friend or Foe) Identification scheme as this scheme is most widely used.

Before you begin

You must have either the Super Admin or System Admin administrator role assigned.

If you have both a primary and a secondary Cisco ISE node, you must log in to the user interface of the secondary node and configure the system time and NTP server settings on each Cisco ISE node in your deployment individually.

Step 1  Choose Administration > System > Settings > System Time.
Step 2  Enter unique IP addresses (IPv4/IPv6/FQDN) for your NTP servers.
Step 3  Check the Only allow authenticated NTP servers check box if you want to restrict Cisco ISE to use only authenticated NTP servers to keep system and network time.
Step 4  (Optional) If you want to authenticate the NTP server using private keys, click the NTP Authentication Keys tab and specify one or more authentication keys if any of the servers that you specify requires authentication via an authentication key, as follows:
   a) Click Add.
b) Enter the necessary **Key ID** and **Key Value**, specify whether the key in question is trusted by activating or deactivating the **Trusted Key** option, and click **OK**. The Key ID field supports numeric values between 1 to 65535 and the Key Value field supports up to 15 alphanumeric characters.

c) Return to the NTP Server Configuration tab when you are finished entering the NTP Server Authentication Keys.

**Step 5** (Optional) If you want to authenticate the NTP server using public-key authentication, configure Autokey on Cisco ISE from the command-line interface (CLI). See the **ntp server** and **crypto** commands in the Cisco Identity Services Engine CLI Reference Guide for your release of ISE for more details.

**Step 6** Click **Save**.

---

### Changing the System Time Zone

Once set, you cannot edit the time zone from the Admin portal. To change the time zone setting, you must enter the following command in the Cisco ISE CLI:

```
clock timezone timezone
```

#### Note

Cisco ISE uses POSIX-style signs in the time zone names and the output abbreviations. Therefore, zones west of Greenwich have a positive sign and zones east of Greenwich have a negative sign. For example, `TZ='Etc/GMT+4'` corresponds to 4 hours behind Universal Time (UT).

#### Caution

Changing the time zone on a Cisco ISE appliance after installation requires ISE services to be restarted on that particular node. Hence we recommend that you perform such changes within a maintenance window. Also, it is important to have all the nodes in a single ISE deployment configured to the same time zone. If you have ISE nodes located in different geographical locations or time zones, you should use a global time zone such as UTC on all the ISE nodes.

For more information on the **clock timezone** command, refer to the *Cisco Identity Services Engine CLI Reference Guide*.

---

### Configure SMTP Server to Support Notifications

You must set up a Simple Mail Transfer Protocol (SMTP) server to send e-mail notifications for alarms, to enable sponsors to send email notification to guests with their login credentials and password reset instructions, and to enable guests to automatically receive their login credentials after they successfully register themselves and with actions to take before their guest accounts expire.

**Step 1** Choose **Administration > System > Settings > SMTP Server**.

**Step 2** Choose **Settings > SMTP Server**.

**Step 3** Enter the host name of the outbound SMTP server in the **SMTP server** field. This SMTP host server must be accessible from the Cisco ISE server. The maximum length for this field is 60 characters.
Step 4  Choose one of these options:

- **Use email address from Sponsor** to send guest notification e-mail from the e-mail address of the sponsor and choose Enable Notifications.

- Use Default email address to specify a specific e-mail address from which to send all guest notifications and enter it in the Default email address field.

Step 5  Click Save.

The recipient of alarm notifications can be any internal admin users with “Include system alarms in emails” option enabled. The sender’s email address for sending alarm notifications is hardcoded as ise@<hostname>.

**Cisco ISE Deployment Upgrade**

Cisco ISE offers a GUI-based centralized upgrade from the Admin portal. The upgrade process is much simplified and the progress of the upgrade and the status of the nodes are displayed on screen. Refer to the Cisco Identity Services Engine Upgrade Guide for a list of pre and post upgrade tasks.

The Upgrade Overview page lists all the nodes in your deployment, the personas that are enabled on them, the version of ISE installed, and the status (indicates whether a node is active or inactive) of the node. You can begin upgrade only if the nodes are in the Active state.

**Different Types of Deployment**

- **Standalone Node**—A single Cisco ISE node assuming the Administration, Policy Service, and Monitoring persona.

- **Multi-Node Deployment**—A distributed deployment with several ISE nodes. The procedure to upgrade a distributed deployment is discussed in detail below.

**ISE Community Resource**

For information on how to assess the network for ISE deployment readiness, see ISE Deployment Assistant (IDA).

**Upgrade a Distributed Deployment**

You can upgrade all the nodes in a Cisco ISE deployment from the Admin portal.

**Note**

The GUI-based upgrade is applicable only if you are upgrading from Release 2.0 or later to a higher release or if you are upgrading a Limited Availability Release of Cisco ISE 2.0 or later to the General Availability Release.

**Before you begin**

Ensure that you have performed the following tasks before you upgrade:

---
- Obtain a backup of the ISE configuration and operational data.
- Obtain a backup of the system logs.
- Disable scheduled backups. Reconfigure the backup schedules after deployment upgrade is complete.
- Export the certificates and private keys.
- Configure a repository. Download the upgrade bundle and place it in the repository.
- Make a note of Active Directory join credentials and RSA SecurID node secret, if applicable. You need this information to connect to Active Directory or RSA SecurID server after upgrade.
- Purge the operational data to improve upgrade performance.

**Step 1**
Click the **Upgrade** tab in the Admin portal.

**Step 2**
Click **Proceed**.

The **Review Checklist** window appears. Read the given instructions carefully.

**Step 3**
Check the **I have reviewed the checklist** check box, and click **Continue**.

The **Download Bundle to Nodes** window appears.

**Step 4**
Download the upgrade bundle from the repository to the nodes:

a) Check the check box next to the nodes to which you want to download the upgrade bundle.

b) Click **Download**.

The **Select Repository and Bundle** window appears.

c) Select the repository.

You can select the same repository or different repositories on different nodes, but you must select the same upgrade bundle on all the nodes.

*Figure 1: Upgrade Window Showing the Repositories Selected for Each Node*

... 

**Step 5**
Click **Continue**.

Once the bundle is downloaded to the node, the node status changes to **Ready for Upgrade**.
The Upgrade Nodes window appears.

*Figure 2: Upgrade Window Showing the Current Deployment and the New Deployment*

**Step 6**  
Choose the upgrade sequence.

When you move a node to the new deployment, a time estimate for the upgrade is displayed on the Upgrade Nodes window. You can use this information to plan for upgrade and minimize downtime. Use the sequence given below if you have a pair of Administration and Monitoring Nodes, and several Policy Service Nodes.

a) By default, the Secondary Administration Node is listed first in the upgrade sequence. After upgrade, this node becomes the Primary Administration Node in the new deployment.

b) The Primary Monitoring Node is the next one in the sequence to be upgraded to the new deployment.

c) Select the Policy Service Nodes and move them to the new deployment. You can alter the sequence in which the Policy Service Nodes are upgraded.

You can upgrade the Policy Service Nodes in sequence or in parallel. You can select a set of Policy Service Nodes and upgrade them in parallel.

d) Select the Secondary Monitoring Node and move it to the new deployment.

e) Finally, select the Primary Administration Node and move it to the new deployment.

If the Administration Nodes also assume the Monitoring persona, then follow the sequence given in the table below:

<table>
<thead>
<tr>
<th>Node Personas In The Current Deployment</th>
<th>Upgrade Sequence</th>
</tr>
</thead>
</table>
| Secondary Administration/Primary Monitoring Node, Policy Service Nodes, Primary Administration/Secondary Monitoring Node | 1. Secondary Administration/Primary Monitoring Node  
2. Policy Service Nodes  
3. Primary Administration/Secondary Monitoring Node |
| Secondary Administration/Secondary Monitoring Node, Policy Service Nodes, Primary Administration/Primary Monitoring Node | 1. Secondary Administration/Secondary Monitoring Node  
2. Policy Service Nodes  
3. Primary Administration/Primary Monitoring Node |
| Secondary Administration Node, Primary Monitoring Node, Policy Service Nodes, Primary Administration/Secondary Monitoring Node | 1. Secondary Administration Node  
2. Primary Monitoring Node  
3. Policy Service Nodes  
4. Primary Administration/Secondary Monitoring Node |
### Node Personas In The Current Deployment

<table>
<thead>
<tr>
<th>Secondary Administration Node, Secondary Monitoring Node, Policy Service Nodes, Primary Administration/Primary Monitoring Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Sequence</td>
</tr>
<tr>
<td>1. Secondary Administration Node</td>
</tr>
<tr>
<td>2. Secondary Monitoring Node</td>
</tr>
<tr>
<td>3. Policy Service Nodes</td>
</tr>
<tr>
<td>4. Primary Administration/Primary Monitoring Node</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secondary Administration/Primary Monitoring Node, Policy Service Nodes, Secondary Monitoring Node, Primary Administration Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Sequence</td>
</tr>
<tr>
<td>1. Secondary Administration/Primary Monitoring Node</td>
</tr>
<tr>
<td>2. Policy Service Nodes</td>
</tr>
<tr>
<td>3. Secondary Monitoring Node</td>
</tr>
<tr>
<td>4. Primary Administration Node</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secondary Administration/Secondary Monitoring Node, Policy Service Nodes, Primary Monitoring Node, Primary Administration Node</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Sequence</td>
</tr>
<tr>
<td>1. Secondary Administration/Secondary Monitoring Node</td>
</tr>
<tr>
<td>2. Policy Service Nodes</td>
</tr>
<tr>
<td>3. Primary Monitoring Node</td>
</tr>
<tr>
<td>4. Primary Administration Node</td>
</tr>
</tbody>
</table>

### Step 7

Check the **Continue with upgrade on failure** check box if you want to continue with the upgrade even if the upgrade fails on any of the Policy Service Nodes in the upgrade sequence.

This option is not applicable for the Secondary Administration Node and the Primary Monitoring Node. If any one of these nodes fail, the upgrade process is rolled back. If any of the Policy Service Nodes fail, the Secondary Monitoring Node and the Primary Administration Node are not upgraded and remain in the old deployment.

### Step 8

Click **Upgrade** to begin the deployment upgrade.

*Figure 3: Upgrade Window Showing the Upgrade Progress*

The upgrade progress is displayed for each node. On successful completion, the node status changes to **Upgrade Complete**.

**Note**  
When you upgrade a node from the Admin portal, if the status does not change for a long time (and remains at 80%), you can check the upgrade logs from the CLI or the status of the upgrade from the console. Log in to the CLI or view the console of the Cisco ISE node to view the progress of upgrade. You can use the **show logging application** command to view the *upgrade-uibackend-cliconsole.log* and *upgrade-postosupgrade-yyyyymmdd-yyyyyyyy.log*. 
If the posture data update process is running on the Primary Administration Node in the new deployment, you cannot register a node to the Primary Administration Node. You can either wait till the posture update process is over (which might take approximately 20 minutes) or disable the posture auto-update feature from the Administration > System > Settings > Posture > Updates page while upgrading or registering a node to the new deployment.

**Note**
Cisco ISE Software Patches

Cisco ISE software patches are usually cumulative. Cisco ISE allows you to perform patch installation and rollback from CLI or GUI.

You can install patches on Cisco ISE servers in your deployment from the Primary PAN. To install a patch from the Primary PAN, you must download the patch from Cisco.com to the system that runs your client browser.

If you are installing the patch from the GUI, the patch is automatically installed on the Primary PAN first. The system then installs the patch on the other nodes in the deployment in the order listed in the GUI. You cannot control the order in which the nodes are updated.

If you are installing the patch from the CLI, you can control the order in which the nodes are updated. However, we recommend that you install the patch on the Primary PAN first.

If you want to validate the patch on some of the nodes before upgrading the entire deployment, you can use the CLI to install the patch on selected nodes. Use the following CLI command to install the patch:

```
patch install <patch_bundle> <repository_that_stores_patch_file>
```

For more information, see the *Cisco Identity Services Engine CLI Reference Guide*.

You can install the required patch version directly. For example, if you are currently using Cisco ISE 2.x and would like to install Cisco ISE 2.x patch 5, you can directly install Cisco ISE 2.x patch 5, without installing the previous patches (in this example, Cisco ISE 2.x patches 1 – 4).

**Related Topics**

- Software Patch Installation Guidelines, on page 87
- Install a Software Patch, on page 88
- Software Patch Installation Guidelines, on page 87
- Software Patch Rollback Guidelines, on page 89
- Install a Software Patch, on page 88
- Roll Back Software Patches, on page 88

**Software Patch Installation Guidelines**

When you install a patch on an ISE node, the node is rebooted after the installation is complete. You might have to wait for a few minutes before you can log in again. You can schedule patch installations during a maintenance window to avoid temporary outage.

Ensure that you install patches that are applicable for the Cisco ISE version that is deployed in your network. Cisco ISE reports any mismatch in versions as well as any errors in the patch file.
You cannot install a patch with a version that is lower than the patch that is currently installed on Cisco ISE. Similarly, you cannot roll back changes of a lower-version patch if a higher version is currently installed on Cisco ISE. For example, if patch 3 is installed on your Cisco ISE servers, you cannot install or roll back patch 1 or 2.

When you install a patch from the Primary PAN that is part of a distributed deployment, Cisco ISE installs the patch on the primary node and then all the secondary nodes in the deployment. If the patch installation is successful on the Primary PAN, Cisco ISE then continues patch installation on the secondary nodes. If it fails on the Primary PAN, the installation does not proceed to the secondary nodes. However, if the installation fails on any of the secondary nodes for any reason, it still continues with the next secondary node in your deployment.

When you install a patch from the Primary PAN that is part of a two-node deployment, Cisco installs the patch on the primary node and then on the secondary node. If the patch installation is successful on the Primary PAN, Cisco then continues patch installation on the secondary node. If it fails on the Primary PAN, the installation does not proceed to the secondary node.

Install a Software Patch

Before you begin

- You must have the Super Admin or System Admin administrator role assigned.

---

**Step 1** Choose Administration > System > Maintenance > Patch Management > Install.

**Step 2** Click Browse and choose the patch that you downloaded from Cisco.com.

**Step 3** Click Install to install the patch.

After the patch is installed on the PAN, Cisco ISE logs you out and you have to wait for a few minutes before you can log in again.

**Note** When patch installation is in progress, Show Node Status is the only function that is accessible on the Patch Management page.

**Step 4** Choose Administration > System > Maintenance > Patch Management to return to the Patch Installation page.

**Step 5** Click the radio button next to the patch that you have installed on any secondary node and click Show Node Status to verify whether installation is complete.

---

**What to do next**

If you need to install the patch on one or more secondary nodes, ensure that the nodes are up and repeat the process to install the patch on the remaining nodes.

Roll Back Software Patches

When you roll back a patch from the PAN that is part of a deployment with multiple nodes, Cisco ISE rolls back the patch on the primary node and then all the secondary nodes in the deployment.
Before you begin

- You must have either the Super Admin or System Admin administrator role assigned.

Step 1  Choose Administration > System > Maintenance > Patch Management.
Step 2  Click the radio button for the patch version whose changes you want to roll back and click Rollback.

**Note** When a patch rollback is in progress, Show Node Status is the only function that is accessible on the Patch Management page.

After the patch is rolled back from the PAN, Cisco ISE logs you out and you have to wait a few minutes before you can log in again.

Step 3  After you log in, click the Alarms link at the bottom of the page to view the status of the rollback operation.
Step 4  Choose Administration > System > Maintenance > Patch Management.
Step 5  To view the progress of the patch rollback, choose the patch in the Patch Management page and click Show Node Status.
Step 6  Click the radio button for the patch and click Show Node Status on a secondary node to ensure that the patch is rolled back from all the nodes in your deployment.

If the patch is not rolled back from any of the secondary nodes, ensure that the node is up and repeat the process to roll back the changes from the remaining nodes. Cisco ISE only rolls back the patch from the nodes that still have this version of the patch installed.

**Related Topics**

Software Patch Rollback Guidelines, on page 89

**Software Patch Rollback Guidelines**

To roll back a patch from Cisco ISE nodes in a deployment, you must first roll back the change from the PAN. If this is successful, the patch is then rolled back from the secondary nodes. If the rollback process fails on the PAN, the patches are not rolled back from the secondary nodes. However, if the patch rollback fails on any secondary node, it still continues to roll back the patch from the next secondary node in your deployment.

While Cisco ISE rolls back the patch from the secondary nodes, you can continue to perform other tasks from the PAN GUI. The secondary nodes will be restarted after the rollback.

**View Patch Install and Rollback Changes**

To view reports related to installed patches, perform the following steps.

**Before you begin**

You must have either the Super Admin or System Admin administrator role assigned. You can install or rollback patches in the Administration > System > Maintenance > Patch Management page. You can also view the status (installed/in-progress/not installed) of a particular patch on each node in the deployment, by selecting a specific patch and clicking the Show Node Status button.
Choose **Operations > Reports > Audit > Operations Audit**. By default, records for the last seven days are displayed.

Click the **Filter** drop-down, and choose **Quick Filter** or **Advanced Filter** and use the required keyword, for example, patch install initiated, to generate a report containing the installed patches.

---

### FIPS Mode Support

Cisco Identity Services Engine uses embedded FIPS 140-2 validated cryptographic modules. For details of the FIPS compliance claims, see the [FIPS Compliance Letter](#).

When the FIPS mode is enabled, the Cisco ISE administrator interface displays a FIPS mode icon at the left of the node name in the upper-right corner of the page.

If Cisco ISE detects the use of a protocol or certificate that is not supported by the FIPS 140-2 standard, it displays a warning with the name of the protocol or certificate that is noncompliant, and the FIPS mode is not enabled. Ensure that you choose only FIPS-compliant protocols and replace non-FIPS compliant certificates before you enable the FIPS mode.

The FIPS standard places limitations on the use of certain algorithms. Cisco ISE enables FIPS 140-2 compliance via RADIUS shared secret and key management measures. When the FIPS mode is enabled, any function that uses non-FIPS compliant algorithms will fail.

The certificates installed in Cisco ISE must be re-issued if the encryption method used in the certificates is not supported by FIPS.

When you enable the FIPS mode, the following functions are affected:

- IEEE 802.1X environment
  - EAP-Flexible Authentication via Secure Tunneling (EAP-FAST)
  - EAP-Transport Layer Security (EAP-TLS)
  - PEAP
  - RADIUS

**Note**

Other protocols like EAP-Message Digest 5 (EAP-MD5), Lightweight Extensible Authentication Protocol (LEAP), and PAP are not compatible with FIPS 140-2 standards and are disabled when the FIPS mode is enabled. Local Web Authentication (LWA), a legacy method of guest access uses PAP and will not work when the FIPS mode is enabled. However, if Host Lookup is used in Allowed Protocols for MAC Authentication Bypass (MAB), guess access with Central Web Authentication (CWA) will work.

- Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL)
- Cisco ISE enables FIPS 140-2 compliance via RADIUS shared secret and key management measures. When the FIPS mode is enabled, any function that uses non-FIPS compliant algorithm will fail.
Guest is not supported in FIPS mode. Enabling FIPS mode also automatically disables Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) protocols, which the guest login function of Cisco ISE requires.

After you enable the FIPS mode, you must reboot all other nodes in the deployment. To minimize disruption to your network, Cisco ISE automatically performs a rolling restart by first restarting the Primary PAN and then restarting each secondary node, one at a time.

**Tip**

We recommend that you do not enable FIPS mode before completing any database migration process.

---

**Enable FIPS Mode in Cisco ISE**

To enable the FIPS mode:

**Step 1** Choose *Administration* > *System* > *Settings* > *FIPS Mode*.

**Step 2** Choose the *Enabled* option from the *FIPS Mode* drop-down list.

**Step 3** Click *Save* and restart your machine.

---

**What to do next**

After you enable FIPS mode, enable and configure the following FIPS 140-2 compliant functions:

- Import Network Devices into Cisco ISE, on page 211
- Generate a Self-Signed Certificate, on page 148
- Create a Certificate Signing Request and Submit the CSR to a Certificate Authority, on page 156
- Configure RADIUS authentication settings under Network Device Definition Settings, on page 988.

In addition, you may want to enable administrator account authorization using a Common Access Card (CAC) function. Although using CAC functions for authorization is not strictly a FIPS 140-2 requirement, it is a well-known secure-access measure that is used in a number of environments to bolster FIPS 140-2 compliance.

---

**Configure Cisco ISE for Administrator CAC Authentication**

**Before you begin**

Before beginning configuration, do the following:

- (Optional) Turn on FIPS mode. FIPS mode is not required for certificate-based authentication, but the two security measures often go hand-in-hand. If you do plan to deploy Cisco ISE in a FIPS 140-2 compliant deployment and to use CAC certificate-based authorization as well, be sure to turn FIPS mode on and specify the appropriate private keys and encryption/decryption settings first.

- Ensure that the domain name server (DNS) in Cisco ISE is set for Active Directory.

- Ensure that Active Directory user and user group membership has been defined for each administrator certificate.
To ensure that Cisco ISE can authenticate and authorize an administrator based on the CAC-based client certificate that is submitted from the browser, be sure that you have configured the following:

- The external identity source (Active Directory in the following example)
- The user groups in Active Directory to which the administrator belongs
- How to find the user's identity in the certificate
- Active Directory user groups to Cisco ISE RBAC permissions mapping
- The Certificate Authority (trust) certificates that sign the client certificates
- A method to determine if a client certificate has been revoked by the CA

You can use a Common Access Card (CAC) to authenticate credentials when logging into Cisco ISE.

---

**Step 1**
Enable FIPS mode. You will be prompted to restart your system after you enable the FIPS mode. You can defer the restart if you are going to import CA certificates as well.

**Step 2**
Configure an Active Directory identity source in Cisco ISE and join all Cisco ISE nodes to Active Directory.

**Step 3**
Configure a certificate authentication profile according to the guidelines.

Be sure to select the attribute in the certificate that contains the administrator user name in the Principal Name X.509 Attribute field. (For CAC cards, the Signature Certificate on the card is normally used to look up the user in Active Directory. The Principal Name is found in this certificate in the "Subject Alternative Name" extension, specifically in a field in that extension that is called "Other Name." So the attribute selection here should be "Subject Alternative Name - Other Name.")

If the AD record for the user contains the user's certificate, and you want to compare the certificate that is received from the browser against the certificate in AD, check the Binary Certificate Comparison check box, and select the Active Directory instance name that was specified earlier.

**Step 4**
Enable Active Directory for Password-Based Admin Authentication. Choose the Active Directory instance name that you connected and joined to Cisco ISE earlier.

*Note* You must use password-based authentication until you complete other configurations. Then, you can change the authentication type to client certificate based at the end of this procedure.

**Step 5**
Create an External Administrator Group and map it to an Active Directory Group. Choose Administration > System > Admin Access > Administrators > Admin Groups. Create an external system administrator group.

**Step 6**
Configure an admin authorization policy to assign RBAC permissions to the external admin groups.

*Caution* We strongly recommend that you create an external Super Admin group, map it to an Active Directory group, and configure an admin authorization policy with Super Admin permissions (menu access and data access), and create at least one user in that Active Directory Group. This mapping ensures that at least one external administrator has Super Admin permissions once Client Certificate-Based Authentication is enabled. Failure to do this may lead to situations where the Cisco ISE administrator is locked out of critical functionality in the Admin Portal.

**Step 7**
Choose Administration > System > Certificates > Certificate Store to import certificate authority certificates into the Cisco ISE certificate trust store.

Cisco ISE does not accept a client certificate unless the CA certificates in the client certificate’s trust chain are placed in the Cisco ISE Certificate Store. You must import the appropriate CA certificates in to the Cisco ISE Certificate Store.
a) Click **Browse** to choose the certificate.
b) Check the Trust for client authentication check box.
c) Click **Submit**.

Cisco ISE prompts you to restart all the nodes in the deployment after you import a certificate. You can defer the restart until you import all the certificates. However, after importing all the certificates, you must restart Cisco ISE before you proceed.

**Step 8**
Configure the certificate authority certificates for revocation status verification.

a) Choose **Administration > System > Certificates > OSCP Services**.
b) Enter the name of an OSCP server, an optional description, and the URL of the server.
c) Choose **Administration > System > Certificates > Certificate Store**.
d) For each CA certificate that can sign a client certificate, specify how to do the revocation status check for that CA. Choose a CA certificate from the list and click Edit. On the edit page, choose OCSP and/or CRL validation. If you choose OCSP, choose an OCSP service to use for that CA. If you choose CRL, specify the CRL Distribution URL and other configuration parameters.

**Step 9**
Enable client certificate-based authentication. Choose **Administration > System > Admin Access > Authentication**.

a) Choose Client Certificate Based authentication type on the Authentication Method tab.
b) Choose the certificate authentication profile that you configured earlier.
c) Select the Active Directory instance name.
d) Click **Save**.

Here, you switch from password-based authentication to client certificate-based authentication. The certificate authentication profile that you configured earlier determines how the administrator’s certificate is authenticated. The administrator is authorized using the external identity source, which in this example is Active Directory.

The Principal Name attribute from the certificate authentication profile is used to look up the administrator in Active Directory.

You have now configured Cisco ISE for administrator CAC authentication.

---

**Related Topics**
- Supported Common Access Card Standards, on page 93
- Common Access Card Operation in Cisco ISE, on page 94

**Supported Common Access Card Standards**

Cisco ISE supports U.S. government users who authenticate themselves using Common Access Card (CAC) authentication devices. A CAC is an identification badge with an electronic chip containing a set of X.509 client certificates that identify a particular employee. Access via the CAC requires a card reader into which you insert the card and enter a PIN. The certificates from the card are then transferred into the Windows certificate store, where they are available to applications such as the local browser running Cisco ISE.

Windows Internet Explorer Version 8 and 9 users running the Windows 7 operating system must install the ActiveIdentity ActivClient Version 6.2.0.133 third-party middleware software product for Cisco ISE to interoperate with CAC. For more information on ActiveIdentity security client products, refer to ActivID ActivClient Security Software Datasheet.
Common Access Card Operation in Cisco ISE

The Admin portal can be configured so that your authentication with Cisco ISE is permitted only by using a client certificate. Credentials-based authentication—such as providing a user ID and password—is not permitted. In client certificate authentication, you insert a Common Access Card (CAC) card, enter a PIN and then enter the Cisco ISE Admin portal URL into the browser address field. The browser forwards the certificate to Cisco ISE, and Cisco ISE authenticates and authorizes your login session, based on the contents of the certificate. If this process is successful, you are presented with the Cisco ISE Monitoring and Troubleshooting home page and given the appropriate RBAC permissions.

Securing SSH Key Exchange Using Diffie-Hellman Algorithm

You can configure Cisco ISE to only allow Diffie-Hellman-Group14-SHA1 SSH key exchanges. To do this, you must enter the following commands from the Cisco ISE Command-Line Interface (CLI) Configuration Mode:

```plaintext
service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

Here’s an example:

```
ise/admin#conf t
ise/admin (config)#service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

Configure Cisco ISE to Send Secure Syslog

To configure Cisco ISE to send only TLS-protected secure syslog between the Cisco ISE nodes and to the Monitoring nodes, you must perform the following tasks:

**Before you begin**

- Ensure that all the Cisco ISE nodes in your deployment are configured with appropriate server certificates. If you want your setup to be FIPS 140-2 compliant, the certificate keys must have a key size of 2048 bits or greater.
- Enable the FIPS mode in the Admin portal.
- Ensure that the default network access authentication policy does not allow any version of the SSL protocol. Use the TLS protocol in the FIPS mode along with FIPS-approved algorithms.
- Ensure that all the nodes in your deployment are registered with the Primary PAN. Also, ensure that at least one node in your deployment has the Monitoring persona enabled to function as the secure syslog receiver (TLS server).

**Step 1** Configure secure syslog remote logging target.

**Step 2** Enable Logging Categories to send auditable events to the secure syslog remote logging target.

**Step 3** Disable TCP Syslog and UDP syslog collectors. Only TLS-protected syslog collectors should be enabled.

**Related Topics**

Configure Secure Syslog Remote Logging Target, on page 95
Configure Secure Syslog Remote Logging Target

Cisco ISE system logs are collected and stored by log collectors for various purposes. You must choose the Cisco ISE Monitoring node as your log collector for configuring a secure syslog target.

Step 1 Log in to the Admin portal.
Step 2 Choose Administration > System > Logging > Remote Logging Targets.
Step 3 Click Add.
Step 4 Enter a name for the secure syslog server.
Step 5 Choose Secure Syslog from the Target Type drop-down list.
Step 6 Choose Enabled from the Status drop-down list.
Step 7 Enter the IP address of the Cisco ISE Monitoring node in your deployment.
Step 8 Enter 6514 as the port number. The secure syslog receiver listens on TCP port 6514.
Step 9 Choose the syslog facility code. The default is LOCAL6.
Step 10 Check the Buffer Messages When Server is Down check box. If this option is checked, Cisco ISE stores the logs if the secure syslog receiver is unreachable, periodically checks the secure syslog receiver, and forwards them when the secure syslog receiver comes up.
   a) Enter the buffer size.
   b) Enter the Reconnect Timeout in seconds for Cisco ISE to periodically check the secure syslog receiver.
Step 11 Select a CA certificate that you want Cisco ISE to present to the secure syslog server.
Step 12 Uncheck the Ignore Server Certificate validation check box. You must not check this option.
Step 13 Click Submit.

Enable Logging Categories to Send Auditable Events to the Secure Syslog Target

You must enable logging categories for Cisco ISE to send auditable events to the secure syslog target.

Step 1 Log in to the Admin portal.
Step 2 Choose Administration > System > Logging > Logging Categories.
Step 3 Click the radio button next to the AAA Audit logging category, then click Edit.
Step 4 Choose WARN from the Log Severity Level drop-down list.
Step 5 Move the secure syslog remote logging target that you created earlier to the Selected box.
Step 6 Click Save.
Step 7 Repeat this procedure to enable the following logging categories:
   • Administrative and Operational Audit
Disable the TCP Syslog and UDP Syslog Collectors

For Cisco ISE to send only secure syslog between the ISE nodes, you must disable the TCP and UDP syslog collectors, and enable only the secure syslog collector.

**Step 1** Log in to the Admin portal.

**Step 2** Choose Administration > System > Logging > Remote Logging Targets.

**Step 3** Click the radio button next to the TCP or UDP syslog collector.

**Step 4** Click Edit.

**Step 5** Choose Disabled from the Status drop-down list.

**Step 6** Click Save.

**Step 7** Repeat this process until you disable all the TCP or UDP syslog collectors.

Default Secure Syslog Collector

Cisco ISE provides default secure syslog collectors for the MnT nodes. By default, no logging categories are mapped to these default secure syslog collectors. The default secure syslog collectors are named as follows:

- Primary MnT node—SecureSyslogCollector
- Secondary MnT node—SecureSyslogCollector2

You can view this information on the Remote Logging Targets page (Administration > System > Logging). You cannot delete the default syslog collectors and cannot update the following fields for the default syslog collectors: Name, Target type, IP/Host address, and Port.

During a fresh Cisco ISE installation, "Default Self-signed Server Certificate" from the system will be added to the Trust Store and marked for “Trust for Client authentication and Syslog” usage, thereby making it available for secure syslog usage. While configuring your deployment or updating the certificates, you must assign relevant certificates to the secure syslog targets.

During upgrade if there are any existing secure syslog targets pointing to MnT nodes on port 6514, the same name and configuration will be retained, but after upgrade you cannot delete these syslog targets and cannot edit the following fields: Name, Target type, IP/Host address, and Port. If no such targets exist at the time of upgrade, default secure syslog targets will be created similar to fresh installation scenario without any certificate mapping. You can assign relevant certificates to these syslog targets. If you try to map a secure syslog target that is not mapped to any certificate, to a logging category, the following message will be displayed:

```
Please configure the certificate for log_target_name
```
Offline Maintenance

If the maintenance time period is less than an hour, take the ISE node offline and perform the maintenance task. When you bring the node back online, PAN will automatically synchronize all the changes that happened during maintenance time period. If the changes are not synchronized automatically, you can manually synchronize it with the PAN.

If the maintenance time period is more than an hour, de-register the node at the time of maintenance and re-register the node when you add the node back to deployment.

We recommend that you schedule the maintenance at a time period during which the activity is low.

---

**Note**

1. Data replication issue may occur if the queue contains more than 1,000,000 messages or if the ISE node is offline for more than 6 hours.

2. If you are planning to perform maintenance on primary MnT node, we recommend that you take operational backup of the MnT node before performing maintenance activities.
Manage Administrators and Admin Access Policies

- Role-Based Access Control, on page 99
- Cisco ISE Administrators, on page 99
- Cisco ISE Administrator Groups, on page 101
- Administrative Access to Cisco ISE, on page 111

Role-Based Access Control

Cisco ISE allows you to define role-based access control (RBAC) policies that allow or deny certain system-operation permissions to an administrator. These RBAC policies are defined based on the identity of individual administrators or the admin group to which they belong.

To further enhance security and control who has access to the Admin portal, you can:

- Configure administrative access settings based on the IP address of remote clients.
- Define strong password policies for administrative accounts.
- Configure session timeouts for administrative GUI sessions.

Cisco ISE Administrators

Cisco ISE administrators use the Admin portal to:

- Manage deployments, help desk operations, network devices and node monitoring and troubleshooting.
- Manage Cisco ISE services, policies, administrator accounts, and system configuration and operations.
- Change administrator and user passwords.

Administrators can access Cisco ISE through the command-line interface (CLI) or web-based interface. The username and password that you configure during Cisco ISE setup is intended only for administrative access to the CLI. This role is considered to be the CLI-admin user, also known as CLI administrator. By default, the username for the CLI-admin user is admin and the password is defined during setup. There is no default password. This CLI-admin user is known as the default admin user. This default admin user account cannot...
be deleted, but can be edited by other administrator accounts (which includes options to enable, disable, or change password for this account).

You can create an administrator or you can promote an existing user to an administrator role. Administrators can also be demoted to simple network user status by disabling the corresponding administrative privileges. Administrators can be considered as users who have local privileges to configure and operate the Cisco ISE system.

Administrators are assigned to one or more admin groups. These admin groups are pre-defined in the system for your convenience, as described in the following section.

Related Topics
Cisco ISE Administrator Groups, on page 101

Privileges of a CLI Administrator Versus a Web-Based Administrator

A CLI administrator can start and stop the Cisco ISE application, apply software patches and upgrades, reload or shut down the Cisco ISE appliance, and view all system and application logs. Because of the special privileges granted to a CLI administrator, we recommend that you protect the CLI administrator credentials and create web-based administrators for configuring and managing Cisco ISE deployments.

Create a New Cisco ISE Administrator

Cisco ISE administrators need accounts with specific roles assigned to it to perform specific administrative tasks. You can create administrator accounts and assign one or more roles to it based on the administrative tasks that an administrator has to perform.

You can use the Admin Users page to view, create, modify, delete, change the status, duplicate, or search for attributes of Cisco ISE administrators.

Step 1
Choose Administration > System > Admin Access > Administrators > Admin Users > Add.

Step 2
Choose one of the following:

• Create New User

  If you choose Create New User, a blank Admin User page appears that you must configure.

• Select from Network Access Users

  If you choose Select from Network Access Users, a list of current users appears from which you can click to choose a user, and the corresponding Admin User page appears.

Step 3
Enter values for the Administrator fields. Supported characters for the name field are # $ ’ ( ) + - ./ @ _.

Step 4
Click Submit to create the new administrator in the Cisco ISE internal database.

Related Topics
The Read-Only Admin Policy, on page 115
Create an Internal Read-Only Admin, on page 123
Customize Menu Access for the Read-Only Administrator, on page 115
Map External Groups to the Read-Only Admin Group, on page 123
Cisco ISE Administrator Groups

Administrator groups, also called as role-based access control (RBAC) groups in Cisco ISE, contain a number of administrators who belong to the same administrative group. All administrators who belong to the same group share a common identity and have the same privileges. An administrator’s identity as a member of a specific administrative group can be used as a condition in authorization policies. An administrator can belong to more than one administrator group.

Regardless of the level of access, any administrator account can modify or delete objects for which it has permission, on any page that the administrator can access.

The Cisco ISE security model limits administrators to creating administrative groups that contain the same set of privileges that the administrator has, which is based on the administrative role of the user as defined in the Cisco ISE database. In this way, administrative groups form the basis for defining privileges for accessing the Cisco ISE systems.

The following table lists the admin groups that are predefined in Cisco ISE and the tasks that members from these groups can perform.

Table 4: Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions

<table>
<thead>
<tr>
<th>Admin Group Role</th>
<th>Access Level</th>
<th>Permissions</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customization Admin</td>
<td>Manage sponsor, guest, and personal</td>
<td>• Configure guest and sponsor access.</td>
<td>• Cannot perform any policy management or identity management or system-level configuration tasks in Cisco ISE</td>
</tr>
<tr>
<td></td>
<td>devices portals</td>
<td>• Manage guest access settings.</td>
<td>• Cannot view any reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Customize end-user web portals.</td>
<td></td>
</tr>
<tr>
<td>Helpdesk Admin</td>
<td>Query monitoring and troubleshooting</td>
<td>• Run all reports</td>
<td>Cannot create, update, or delete reports, troubleshooting flows, live authentications, or alarms</td>
</tr>
<tr>
<td></td>
<td>operations</td>
<td>• Run all troubleshooting flows</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View the Cisco ISE dashboard and livelogs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View alarms</td>
<td></td>
</tr>
<tr>
<td>Admin Group Role</td>
<td>Access Level</td>
<td>Permissions</td>
<td>Restrictions</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Identity Admin</td>
<td>• Manage user accounts and endpoints • Manage identity sources</td>
<td>• Add, edit, and delete user accounts and endpoints</td>
<td>Cannot perform any policy management or system-level configuration tasks in Cisco ISE</td>
</tr>
<tr>
<td>MnT Admin</td>
<td>Perform all monitoring and troubleshooting operations.</td>
<td>• Manage all reports (run, create, and delete)</td>
<td>Cannot perform any policy management or identity management or system-level configuration tasks in Cisco ISE</td>
</tr>
<tr>
<td>Admin Group Role</td>
<td>Access Level</td>
<td>Permissions</td>
<td>Restrictions</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Network Device Admin       | Manage Cisco ISE network devices and network device repository. | • Read and write permissions on network devices  
                              |                                                                 | • Read and write permissions on NDGs and all network resources object types  
                              |                                                                 | • View the Cisco ISE dashboard, livelogs, alarms, and reports  
                              |                                                                 | • Run all troubleshooting flows  
<pre><code>                          |                                                                 | Cannot perform any policy management or identity management or system-level configuration tasks in Cisco ISE |
</code></pre>
<table>
<thead>
<tr>
<th>Admin Group Role</th>
<th>Access Level</th>
<th>Permissions</th>
<th>Restrictions</th>
</tr>
</thead>
</table>
| Policy Admin         | Create and manage policies for all Cisco ISE services across the network that are related to authentication, authorization, posture, profiler, client provisioning, and work centers. | • Read and write permissions on all the elements used in policies, such as authorization profiles, NDGs, and conditions.  
• Read and write permissions on identities, endpoints, and identity groups (user identity groups and endpoint identity groups).  
• Read and write permissions on services policies and settings.  
• View the Cisco ISE dashboard, livelogs, alarms, and reports.  
• Run all troubleshooting flows.  
• Device Administration—Access to device administration work centers. Permission for TACACS Policy Conditions and results. Network Device permissions for TACACS proxy and proxy sequences. | Cannot perform any identity management or system-level configuration tasks in Cisco ISE.  
Device Administration—Access to the work center does not guarantee access to the subordinate links. |
<table>
<thead>
<tr>
<th>Admin Group Role</th>
<th>Access Level</th>
<th>Permissions</th>
<th>Restrictions</th>
</tr>
</thead>
</table>
| RBAC Admin       | All tasks under the Operations menu except for the Endpoint Protection Services Adaptive Network Control, and partial access to some menu items under Administration | • View the authentication details  
• Enable or disable Endpoint Protection Services Adaptive Network Control  
• Create, edit, and delete alarms; generate and view reports; and use Cisco ISE to troubleshoot problems in your network  
• Read permissions on administrator account settings and admin group settings  
• View permissions on admin access and data access permissions along with the RBAC policy page.  
• View the Cisco ISE dashboard, livelogs, alarms, and reports  
• Run all troubleshooting flows | Cannot perform any identity management or system-level configuration tasks in Cisco ISE |
<table>
<thead>
<tr>
<th>Admin Group Role</th>
<th>Access Level</th>
<th>Permissions</th>
<th>Restrictions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read-Only Admin</td>
<td>Read-only access to</td>
<td>• View and use the functions of the dashboard, reports, and livelogs/sessions, such as filtering data, querying, saving options, printing, and exporting data.</td>
<td>• Change passwords of their own accounts.</td>
</tr>
<tr>
<td></td>
<td>the ISE GUI.</td>
<td>• Query ISE using global search, reports, and livelog/sessions.</td>
<td>• Query ISE using global search, reports, and livelog/sessions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Filter and save data based on the attributes.</td>
<td>• Filter and save data based on the attributes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Export data pertaining to authentication policies, profile policies, users, endpoints, network devices, network device groups, identities (including groups), and other configurations.</td>
<td>• Export data pertaining to authentication policies, profile policies, users, endpoints, network devices, network device groups, identities (including groups), and other configurations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Customize report queries, save, print, and export them.</td>
<td>• Customize report queries, save, print, and export them.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Generate custom report queries, save, print, or export the results.</td>
<td>• Generate custom report queries, save, print, or export the results.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Save UI settings for future reference.</td>
<td>• Save UI settings for future reference.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Download logs, such as ise-psc-log from the Operations &gt; Troubleshoot &gt; Download Logs page.</td>
<td>• Download logs, such as ise-psc-log from the Operations &gt; Troubleshoot &gt; Download Logs page.</td>
</tr>
<tr>
<td>Admin Group Role</td>
<td>Access Level</td>
<td>Permissions</td>
<td>Restrictions</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Perform any configuration changes such as create, update, delete, import, quarantine, and MDM actions of any objects, such as authorization policies, authentication policies, posture policies, profiler policies, endpoints, and users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Perform any system operations, such as backup/restore, registration/deregistration of nodes, sync-up of nodes, creating, editing and deleting of node groups, or upgrade/installation of patches.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Import data pertaining to policies, network devices, network device groups, identities (including groups), and other configurations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Perform operations, such as CoA, endpoint debugging, modifying collection filters, bypassing suppression on live sessions data, modifying the PAN-HA failover settings, and editing the personas or services of any Cisco ISE node.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Run commands that</td>
</tr>
<tr>
<td>Admin Group Role</td>
<td>Access Level</td>
<td>Permissions</td>
<td>Restrictions</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Super Admin</td>
<td>All Cisco ISE administrative functions. The default administrator account belongs to this group.</td>
<td>Create, read, update, delete, and eXecute (CRUDX) permissions on all Cisco ISE resources. <strong>Note</strong> The super admin user cannot modify the default system-generated RBAC policies and permissions. To do this, you must create new RBAC policies with the necessary permissions based on your needs, and map these policies to any admin group.</td>
<td>Device Administration—Access to device administration work centers. Permission for TACACS Policy Conditions and results. Network Device permissions for TACACS proxy and proxy sequences. In addition, permission to enable TACACS global protocol settings.</td>
</tr>
<tr>
<td>Admin Group Role</td>
<td>Access Level</td>
<td>Permissions</td>
<td>Restrictions</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| System Admin     | All Cisco ISE configuration and maintenance tasks. | Full access (read and write permissions) to perform all activities under the Operations tab and partial access to some menu items under the Administration tab.  
  • Read permissions on administrator account settings and administrator group settings  
  • Read permissions on admin access and data access permissions along with the RBAC policy page  
  • Read and write permissions for all options under the Administration > System menu  
  • View the authentication details  
  • Enable or disable Endpoint Protection Services Adaptive Network Control  
  • Create, edit, and delete alarms; generate and view reports; and use Cisco ISE to troubleshoot problems in your network  
  • Device Administration—Permission to enable TACACS global protocol settings. | Cannot perform any policy management or system-level configuration tasks in Cisco ISE |
### Admin Group Role | Access Level | Permissions | Restrictions
--- | --- | --- | ---
External RESTful Services (ERS) Admin | Full access to all ERS API requests such as GET, POST, DELETE, PUT | • Create, Read, Update, and Delete ERS API requests | The role is meant only for ERS authorization supporting Internal Users, Identity Groups, Endpoints, Endpoint Groups, and SGT
External RESTful Services (ERS) Operator | Read-only access to ERS API, only GET | • Can only Read ERS API requests | The role is meant only for ERS authorization supporting Internal Users, Identity Groups, Endpoints, Endpoint Groups, and SGT
TACACS+ Admin | Full access | Access to the:  
• Device Administration Work Center.  
• Deployment—To enable TACACS+ services.  
• External Identity Stores.  
• Operations > TACACS Live Logs page. | —

**Related Topics**
Cisco ISE Administrators, on page 99

## Create Admin Groups

The Admin Groups page allows you to view, create, modify, delete, duplicate, or filter Cisco ISE network admin groups.

**Before you begin**

To configure an external administrator group type, you must have already specified one or more external identity stores.

**Step 1**  
Choose Administration > System > Admin Access > Administrators > Admin Groups.

**Step 2**  
Click **Add**, and enter a Name and Description. Supported special characters for the name field are: space, # $ & ‘ ( ) * + - . / @ _ .

**Step 3**  
Specify the Type of administrator group you are configuring:
• Internal—Administrators assigned to this group type will authenticate against the credentials that are stored in the Cisco ISE internal database.

• External—Administrators that you assign to this group will authenticate against the credentials that are contained in the external identity store that you specify in the attribute selector. After choosing External, specify the identity store from which Cisco ISE should import the external group information.

**Step 4**  
Click Add to add users to the Admin Group Users table. From the Users list, select the users to be added to the admin group.

**Step 5**  
To delete users from the Admin Group Users table, check the check box corresponding to the user that you want to delete, and click Remove.

**Step 6**  
Click Submit to save any changes made to the admin group that you created in the Cisco ISE database.

---

**Note**  
If an internal user is configured with an external identity store for authentication, while logging in to the ISE Admin portal, the internal user must select the external identity store as the Identity Source. Authentication will fail if Internal Identity Source is selected.

### Administrative Access to Cisco ISE

Cisco ISE administrators can perform various administrative tasks based on the administrative group to which they belong. These administrative tasks are critical and you must ensure that administrative access is restricted to users who are authorized to administer Cisco ISE in your network.

Cisco ISE allows you to control administrative access to its web interface through the following options:

#### Role-Based Access Control in Cisco ISE

Role-based access control policies (known as admin access) are access control policies that you define to provide limited access to the Cisco ISE administrative interface. These admin access policies allow you to customize the amount and type of access on a per-administrator or per-admin group basis using specified role-based access permission settings that apply to an individual admin user or an admin group.

Role-based access determines what each entity can access, which is controlled with an access control policy. Role-based access also determines the administrative role that is in use, the admin group to which the entity belongs, and the corresponding permissions and settings that are applied based upon the role of the entity.

#### Role-Based Permissions

Cisco ISE allows you to configure permissions at the menu and data levels, called the menu access and data access permissions.

The menu access permissions allow you to show or hide the menu and submenu items of the Cisco ISE administrative interface. This feature lets you create permissions so that you can restrict or enable access at the menu level.
The data access permissions allow you to grant read/write, read only, or no access to the following data in the Cisco ISE interface: Admin Groups, User Identity Groups, Endpoint Identity Groups, Locations, and Device Types.

**RBAC Policies**

RBAC policies determine if an administrator can be granted a specific type of access to a menu item or other identity group data elements. You can grant or deny access to a menu item or identity group data element to an administrator based on the admin group by using RBAC policies. When administrators log in to the Admin portal, they can access menus and data that are based on the policies and permissions defined for the admin groups with which they are associated.

RBAC policies map admin groups to menu access and data access permissions. For example, you can prevent a network administrator from viewing the Admin Access operations menu and the policy data elements. This can be achieved by creating a custom RBAC policy for the admin group with which the network administrator is associated.

*Note*
If you are using customized RBAC policies for admin access, ensure that you provide all relevant menu access for a given data access. For example, to add or delete endpoints with data access of Identity or Policy Admin, you must provide menu access to **Work Center > Network Access** and **Administration > Identity Management**.

**Default Menu Access Permissions**

Cisco ISE provides an out of the box set of permissions that are associated with a set of predefined admin groups. Having predefined admin group permissions allow you to set permissions so that a member of any admin group can have full or limited access to the menu items within the administrative interface (known as menu access) and to delegate an admin group to use the data access elements of other admin groups (known as data access). These permissions are reusable entities that can be further used to formulate RBAC policies for various admin groups. Cisco ISE provides a set of system defined menu access permissions that are already used in the default RBAC policies. Apart from the predefined menu access permissions, Cisco ISE also allows you to create custom menu access permissions that you can use in RBAC policies. The key icon represents menu access privileges for the menus and submenus and the key with a close icon represents no access for different RBAC groups.

*Note*
For Super Admin User, all the menu items are available. For other Admin Users, all the Menu Items in this column are available for Standalone deployment and Primary Node in Distributed Deployment. For Secondary Node in Distributed Deployment, the Menu Items under the Administration tab are not available.

**Configure Menu Access Permissions**

Cisco ISE allows you to create custom menu access permissions that you can map to an RBAC policy. Depending on the role of the administrators, you can allow them to access only specific menu options.

**Step 1**
Choose **Administration > System > Admin Access > Authorization > Permissions > Menu Access**.

**Step 2**
Click **Add**, and enter values for the Name and Description fields.
a) Click to expand the menu item up to the desired level, and click the menu item(s) on which you want to create permissions.
b) In the Permissions for Menu Access area, click Show.

Step 3  Click Submit.

---

Prerequisites for Granting Data Access Permissions

When an RBAC admin has Full Access permission to an object (for example, Employee in the User Identity Groups data type), the admin can view, add, update, and delete users who belong to that group. Ensure that the admin has menu access permission granted for the Users page (Administration > Identity Management > Identities > Users). This is applicable for Network Devices and Endpoints objects (based on the permissions granted to the Network Device Groups and Endpoint Identity Groups data types).

You cannot enable or restrict data access for network devices that belong to the default network device group objects—All Device Types and All Locations. All network devices are displayed if Full Access data permission is granted to an object created under these default network device group objects. Therefore, it is recommended that you create a separate hierarchy for the Network Device Groups data type, which is independent of the default network device group objects. You should assign the network device objects to the newly created Network Devices Groups to create restricted access.

Note

You can enable or restrict data access permissions only for the User Identity Groups, Network Device Groups, and Endpoint Identity Groups. It is not applicable for Admin Groups.

---

Default Data Access Permissions

Cisco ISE comes with a set of predefined data access permissions. The data access permissions enable multiple administrators to have the data access permissions within the same user population. You can enable or restrict the use of data access permissions to one or more admin groups. This process allows autonomous delegated control to administrators of one admin group to reuse data access permissions of the chosen admin groups through selective association. Data access permissions range from full access to no access for viewing selected admin groups or the network device groups. RBAC policies are defined based on the administrator (RBAC) group, menu access, and data access permissions. You first create menu access and data access permissions and then create an RBAC policy that associates an admin group with the corresponding menu access and data access permissions. The RBAC policy takes the form: If admin_group=Super Admin then assign SuperAdmin Menu Access permission + SuperAdmin Data Access permission. Apart from the predefined data access permissions, Cisco ISE also allows you to create custom data access permissions that you can associate with an RBAC policy.

There are three data access permissions namely, Full Access, No Access, and Read Only access that can be granted to admin groups.

The Read Only permission can be granted to the following admin groups:

- Administration > Admin Access > Administrators > Admin Groups
- Administration > Groups > User Identity Group
- Administration > Groups > Endpoint Identity Groups
- Network Visibility > Endpoints
If you have Read Only permission on a data type (for example, Endpoint Identity Groups), you will not be able to perform CRUD operations on the data type. If you have Read Only permission on an object (for example, GuestEndpoints), you cannot perform edit/delete operations on the object.

The image below describes how the Data Access Privileges apply at the second- or third-level menu that contains additional submenus or options for different RBAC groups.

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Denotes full access for the User Identity Groups data type.</td>
</tr>
<tr>
<td>2</td>
<td>Denotes that Endpoint Identity Groups derives the maximum permission (full access) that is granted to its child (Asia).</td>
</tr>
<tr>
<td>3</td>
<td>Denotes no access for the object (Blacklist).</td>
</tr>
</tbody>
</table>
Configure Data Access Permissions

Cisco ISE allows you to create custom data access permissions that you can map to an RBAC policy. Based on the role of the administrator, you can choose to provide them access only to select data.

**Table:**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Denotes that the parent (Continents) derives the maximum access permission granted to its child (Asia).</td>
</tr>
<tr>
<td>5</td>
<td>Denotes Read Only access for the object (Australia).</td>
</tr>
<tr>
<td>6</td>
<td>Denotes that when Full Access is granted to the parent (Network Device Groups), it results in the children automatically inheriting permissions.</td>
</tr>
<tr>
<td>7</td>
<td>Denotes that when Full Access is granted to the parent (Asia), it results in the objects inheriting the Full Access permission, unless permissions are explicitly granted to the objects.</td>
</tr>
</tbody>
</table>

**Configure Data Access Permissions**

Cisco ISE allows you to create custom data access permissions that you can map to an RBAC policy. Based on the role of the administrator, you can choose to provide them access only to select data.

**Step 1** Choose Administration > System > Admin Access > Authorization > Permissions.

**Step 2** Choose Permissions > Data Access.

**Step 3** Click Add, and enter values for the Name and Description fields.
   a) Click to expand the admin group and select the desired admin group.
   b) Click Full Access, Read Only Access, or No Access.

**Step 4** Click Save.

**The Read-Only Admin Policy**

The default Read-Only Admin policy is available in the Administration > System > Admin Access > Authorization > Policy page. This policy is available for both new installation and upgraded deployment. The Read-Only Admin policy is applicable to the Read-Only Admin group. By default, Super Admin Menu Access and Read-Only Data Access permissions are granted to Read-Only administrators.

**Note**

The default read-only policy is mapped to the Read Only Admin group. You cannot create custom RBAC policy using the Read Only Admin group.

**Customize Menu Access for the Read-Only Administrator**

By default, Read-Only Administrators are given Super Admin Menu Access and Read Only Admin Data Access. However, if the Super Admin requires that the Read-Only Administrator view only the Home and Administration tabs, the Super Admin can create a custom menu access or customize the default Permissions to, for example, MnT Admin Menu Access or Policy Admin Menu Access. The Super Admin cannot modify the Read Only Data Access mapped to the Read Only Admin Policy.
### Configure Admin Access Policies

An Admin Access (RBAC) policy is represented in an if-then format, where if is the RBAC Admin Group value and then is the RBAC Permissions value.

The RBAC policies page (Administration > System > Admin Access > Authorization > Policy) contains a list of default policies. You cannot edit or delete these default policies. However, you can edit the data access permissions for the Read-Only Admin policy. The RBAC policies page also allows you to create custom RBAC policies for an admin group specifically for your work place, and apply to personalized admin groups.

When you assign limited menu access, make sure that the data access permissions allow the administrator to access the data that is required to use the specified menus. For example, if you give menu access to the MyDevices portal, but don't allow data access to Endpoint Identity Groups, then that administrator cannot modify the portal.

#### Before you begin
- Ensure that you have created all admin groups for which you want to define the RBAC policies.
- Ensure that these admin groups are mapped to the individual admin users.
- Ensure that you have configured the RBAC permissions, such as menu access and data access permissions.

#### Step 1
Choose **Administration > System > Admin Access > Authorization > Policy**.

The RBAC Policies page contains a set of ready-to-use predefined policies for default admin groups. You cannot edit or delete these default policies. However, you can edit the data access permissions for the default Read-Only Admin policy.
Step 2  Click Actions next to any of the default RBAC policy rule.
Here, you can insert new RBAC policies, duplicate an existing RBAC policy, and delete an existing RBAC policy.

Step 3  Click Insert new policy.

Step 4  Enter values for the Rule Name, RBAC Group(s), and Permissions fields.
You cannot select multiple menu access and data access permissions when creating an RBAC policy.

Step 5  Click Save.

---

**Administrator Access Settings**

Cisco ISE allows you to define some rules for administrator accounts to enhance security. You can restrict access to the management interfaces, force administrators to use strong passwords, regularly change their passwords, and so on. The password policy that you define under the Administrator Account Settings in Cisco ISE applies to all administrator accounts.

Cisco ISE does not support administrator passwords with UTF-8 characters.

**Configure the Maximum Number of Concurrent Administrative Sessions and Login Banners**

You can configure the maximum number of concurrent administrative GUI or CLI (SSH) sessions and login banners that help and guide administrators who access your administrative web or CLI interface. You can configure login banners that appear before and after an administrator logs in. By default, these login banners are disabled.

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

---

Step 1  Choose Administration > System > Admin Access > Settings > Access > Session.

Step 2  Enter the maximum number of concurrent administrative sessions that you want to allow through the GUI and CLI interfaces. The valid range for concurrent administrative GUI sessions is from 1 to 20. The valid range for concurrent administrative CLI sessions is 1 to 10.

Step 3  If you want Cisco ISE to display a message before an administrator logs in, check the Pre-login banner check box and enter your message in the text box.

Step 4  If you want Cisco ISE to display a message after an administrator logs in, check the Post-login banner check box and enter your message in the text box.

Step 5  Click Save.

---

**Related Topics**

- Allow Administrative Access to Cisco ISE from Select IP Addresses, on page 117

**Allow Administrative Access to Cisco ISE from Select IP Addresses**

Cisco ISE allows you to configure a list of IP addresses from which administrators can access the Cisco ISE management interfaces.
The administrator access control settings are only applicable for Cisco ISE nodes that assume the Administration, Policy Service, or Monitoring personas. These restrictions are replicated from the primary to the secondary nodes.

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

---

**Step 1** Choose **Administration > System > Admin Access > Settings > Access > IP Access**.

**Step 2** Select **Allow only listed IP addresses to connect**.

**Note** Connection on Port 161 (SNMP) is used for Administrative access. However, when IP Access restrictions are configured, the snmpwalk fails if the node from which it was performed is not configured for Administrative access.

**Step 3** From the Configure IP List for Access Restriction area, click **Add**.

**Step 4** Enter IP addresses in the classless interdomain routing (CIDR) format in the IP address field.

**Note** This IP address can range from IPv4 and IPv6. You can now configure multiple IPv6 addresses for an ISE node.

**Step 5** Enter the subnet mask in the Netmask in CIDR format field.

**Step 6** Click **OK**. Repeat the process to add more IP address ranges to this list.

**Step 7** Click **Save** to save the changes.

**Step 8** Click **Reset** to refresh the **IP Access** page.

---

**Configure a Password Policy for Administrator Accounts**

Cisco ISE also allows you to create a password policy for administrator accounts to enhance security. You can define whether you want a password based or client certificate based administrator authentication. The password policy that you define here is applied to all administrator accounts in Cisco ISE.

**Note** Cisco ISE does not support administrator passwords with UTF-8 characters.

**Before you begin**

- To perform the following task, you must be a Super Admin or System Admin.
- Make sure that the auto-failover configuration, if enabled in your deployment, is turned off. When you change the authentication method, you will be restarting the application server processes. There might be a delay while these services restart. Due to this delay in restart of services, auto-failover of secondary Administration node might get initiated.

---

**Step 1** Choose **Administration > System > Admin Access > Authentication**.

**Step 2** Select either of these authentication methods:
• **Password Based**—If you want to use the standard user ID and password credentials for an administrator login, choose the **Password Based** option and specify either the “Internal” or “External” authentication type.

**Note**  
If you have configured an external identity source such as LDAP and want to use that as your authentication source to grant access to the admin user, you must select that particular identity source from the Identity Source list box.

• **Client Certificate Based**—If you want to specify a certificate-based policy, choose the **Client Certificate Based** option, and select an existing Certificate Authentication Profile.

**Step 3**  
Click the **Password Policy** tab and enter the values.

**Step 4**  
Click **Save** to save the administrator password policy.

**Note**  
If you are using an external identity store to authenticate administrators at login, remember that even if this setting is configured for the password policy applied to the administrator profile, the external identity store will still validate the administrator’s username and password.

---

**Related Topics**

- [Administrator Password Policy Settings](#), on page 947
- [Configure Account Disable Policy for Administrator Accounts](#), on page 119
- [Configure Lock or Suspend Settings for Administrator Accounts](#), on page 119

---

**Configure Account Disable Policy for Administrator Accounts**

Cisco ISE allows you to disable the administrator account if the administrator account is not authenticated for the configured consecutive number of days.

**Step 1**  
Choose **Administration > System > Admin Access > Authentication > Account Disable Policy**.

**Step 2**  
Check the **Disable account after n days of inactivity** check box and enter the number of days.

This option allows you to disable the administrator account if the administrator account was inactive for the consecutive number of days. However, you can exclude individual administrator account from this account disable policy using the **Inactive Account Never Disabled** option available at **Administration > System > Admin Access > Administrators > Admin Users**.

**Step 3**  
Click **Save** to configure the global account disable policy for administrators.

---

**Configure Lock or Suspend Settings for Administrator Accounts**

Cisco ISE allows you to lock or suspend administrator accounts (including password-based Internal Admin accounts and certificate-based Admin accounts) that have more than a specified number of failed login attempts.

**Step 1**  
Choose **Administration > System > Admin Access > Authentication > Lock/Suspend Settings**.

**Step 2**  
Check the **Suspend or Lock Account With Incorrect Login Attempts** check box and enter the number of failed attempts after which action should be taken. The valid range is between 3 and 20.
Configure Session Timeout for Administrators

Cisco ISE allows you to determine the length of time an administration GUI session can be inactive and still remain connected. You can specify a time in minutes after which Cisco ISE logs out the administrator. After a session timeout, the administrator must log in again to access the Cisco ISE Admin portal.

**Before you begin**
To perform the following task, you must be a Super Admin or System Admin.

**Step 1** Choose Administration > System > Admin Access > Settings > Session > Session Timeout.

**Step 2** Enter the time in minutes that you want Cisco ISE to wait before it logs out the administrator if there is no activity. The default value is 60 minutes. The valid range is from 6 to 100 minutes.

**Step 3** Click Save.

Terminate an Active Administrative Session

Cisco ISE displays all active administrative sessions from which you can select any session and terminate at any point of time, if a need to do so arises. The maximum number of concurrent administrative GUI sessions is 20. If the maximum number of GUI sessions is reached, an administrator who belongs to the super admin group can log in and terminate some of the sessions.

**Before you begin**
To perform the following task, you must be a Super Admin.

**Step 1** Choose Administration > System > Admin Access > Settings > Session > Session Info.

**Step 2** Check the check box next to the session ID that you want to terminate and click Invalidate.

Change Administrator Name

Cisco ISE allows you to change your username from the GUI.

**Before you begin**
To perform the following task, you must be a Super Admin or System Admin.
Step 1: Log in to the Admin portal.
Step 2: Click your username that appears as a link at the upper right corner of the Cisco ISE UI.
Step 3: Enter the new username in the Admin User page that appears.
Step 4: Edit any other details about your account that you want to change.
Step 5: Click Save.

Administrative Access to Cisco ISE Using an External Identity Store

In Cisco ISE, you can authenticate administrators via an external identity store such as Active Directory, LDAP, or RSA SecureID. There are two models you can use to provide authentication via an external identity store:

- **External Authentication and Authorization**—There are no credentials that are specified in the local Cisco ISE database for the administrator, and authorization is based on external identity store group membership only. This model is used for Active Directory and LDAP authentication.

- **External Authentication and Internal Authorization**—The administrator’s authentication credentials come from the external identity source, and authorization and administrator role assignment take place using the local Cisco ISE database. This model is used for RSA SecurID authentication. This method requires you to configure the same username in both the external identity store and the local Cisco ISE database.

During the authentication process, Cisco ISE is designed to “fall back” and attempt to perform authentication from the internal identity database, if communication with the external identity store has not been established or if it fails. In addition, whenever an administrator for whom you have set up external authentication launches a browser and initiates a login session, the administrator still has the option to request authentication via the Cisco ISE local database by choosing “Internal” from the Identity Store drop-down selector in the login dialog.

---

**Note**

You can configure this method of providing external administrator authentication only via the Admin portal. The Cisco ISE Command Line Interface (CLI) does not feature these functions.

If your network does not already have one or more existing external identity stores, ensure that you have installed the necessary external identity stores and configured Cisco ISE to access those identity stores.

**External Authentication and Authorization**

By default, Cisco ISE provides internal administrator authentication. To set up external authentication, you must create a password policy for the external administrator accounts that you define in the external identity stores. You can then apply this policy to the external administrator groups that eventually become a part of the external administrator RBAC policy.

In addition to providing authentication via an external identity store, your network may also require you to use a Common Access Card (CAC) authentication device.

To configure external authentication, you must:

- Configure password-based authentication using an external identity store.
• Create an external administrator group.
• Configure menu access and data access permissions for the external administrator group.
• Create an RBAC policy for external administrator authentication.

**External Authentication Process Flow**

When the administrator logs in, the login session passes through the following steps in the process:

1. The administrator sends an RSA SecurID challenge.
2. RSA SecurID returns a challenge response.
3. The administrator enters a user name and the RSA SecurID challenge response in the Cisco ISE login dialog, as if entering the user ID and password.
4. The administrator ensures that the specified Identity Store is the external RSA SecurID resource.
5. The administrator clicks **Login**.

Upon logging in, the administrator sees only the menu and data access items that are specified in the RBAC policy.

**Configure a Password-Based Authentication Using an External Identity Store**

You must first configure password-based authentication for administrators who authenticate using an external identity store such as Active Directory or LDAP.

---

**Step 1** Choose **Administration > System > Admin Access > Authentication**.

**Step 2** On the Authentication Method tab, select **Password Based** and choose one of the external identity sources you should have already configured. For example, the Active Directory instance that you have created.

**Step 3** Configure any other specific password policy settings that you want for administrators who authenticate using an external identity store.

**Step 4** Click **Save**.

---

**Create an External Administrator Group**

You will need to create an external Active Directory or LDAP administrator group. This ensures that Cisco ISE uses the username that is defined in the external Active Directory or LDAP identity store to validate the administrator username and password that you entered upon login.

Cisco ISE imports the Active Directory or LDAP group information from the external resource and stores it as a dictionary attribute. You can then specify that attribute as one of the policy elements when it is time to configure the RBAC policy for this external administrator authentication method.

---

**Step 1** Choose **Administration > System > Admin Access > Administrators > Admin Groups**.

The **External Groups Mapped** column displays the number of external groups that are mapped to internal RBAC roles. You can click the number corresponding to a admin role to view the external groups (for example, if you click 2 displayed against Super Admin, the names of two external groups are displayed).
Step 2  Click Add.
Step 3  Enter a name and optional description.
Step 4  Choose the External radio button.
        If you have connected and joined to an Active Directory domain, your Active Directory instance name appears in the Name field.
Step 5  From the External Groups drop-down list box, choose the Active Directory group that you want to map for this external administrator group.
        Click the “+” sign to map additional Active Directory groups to this external administrator group.
Step 6  Click Save.

Create an Internal Read-Only Admin

Step 1  Choose Administration > System > Admin Access > Administrators > Admin Users.
Step 2  Click Add and select Create An Admin User.
Step 3  Check the Read Only check box to create a Read-Only administrator.

Map External Groups to the Read-Only Admin Group

Step 1  Choose Administration > Identity Management > External Identity Sources to configure the external authentication source. See the Manage Users and External Identity Sources chapter for more information.
Step 2  Click the required external identity source, such as Active Directory or LDAP, and then retrieve the groups from the selected identity source.
Step 3  Choose Administration > System > Admin Access > Authentication to map the authentication method for the admin access with the identity source.
Step 4  Choose Administration > System > Admin Access > Administrators > Admin Groups and select Read Only Admin group.
Step 5  Check the Type External check box and select the required external groups for whom you intend to provide read-only privileges.
Step 6  Click Save.
        An external group that is mapped to a Read-Only Admin group cannot be assigned to any other admin group.

Configure Menu Access and Data Access Permissions for the External Administrator Group

You must configure menu access and data access permissions that can be assigned to the external administrator group.

Step 1  Choose Administration > System > Admin Access > Permissions.
Step 2  Click one of the following:
Create an RBAC Policy for External Administrator Authentication

In order to configure Cisco ISE to authenticate the administrator using an external identity store and to specify custom menu and data access permissions at the same time, you must configure a new RBAC policy. This policy must have the external administrator group for authentication and the Cisco ISE menu and data access permissions to manage the external authentication and authorization.

Note

You cannot modify an existing (system-preset) RBAC policy to specify these new external attributes. If you have an existing policy that you would like to use as a “template,” be sure to duplicate that policy, rename it, and then assign the new attributes.

Step 1 Choose Administration > System > Admin Access > Authorization > Policy.
Step 2 Specify the rule name, external administrator group, and permissions.
Remember that the appropriate external administrator group must be assigned to the correct administrator user IDs. Ensure that the administrator in question is associated with the correct external administrator group.
Step 3 Click Save.

If you log in as an administrator, and the Cisco ISE RBAC policy is not able to authenticate your administrator identity, Cisco ISE displays an “unauthenticated” message, and you cannot access the Admin portal.

Configure Admin Access Using an External Identity Store for Authentication with Internal Authorization

This method requires you to configure the same username in both the external identity store and the local Cisco ISE database. When you configure Cisco ISE to provide administrator authentication using an external RSA SecurID identity store, administrator credential authentication is performed by the RSA identity store. However, authorization (policy application) is still done according to the Cisco ISE internal database. In addition, there are two important factors to remember that are different from external authentication and authorization:

• You do not need to specify any particular external administrator groups for the administrator.
• You must configure the same username in both the external identity store and the local Cisco ISE database.
Step 1  Choose Administration > System > Admin Access > Administrators > Admin Users.

Step 2  Ensure that the administrator username in the external RSA identity store is also present in Cisco ISE. Ensure that you click the External option under Password.

**Note**  You do not need to specify a password for this external administrator user ID, nor are you required to apply any specially configured external administrator group to the associated RBAC policy.

Step 3  Click Save.
This chapter describes the licensing mechanism and schemes that are available for Cisco ISE and how to add and upgrade licenses.

- Cisco ISE Licenses, on page 127
- Manage Traditional License Files, on page 128

Cisco ISE Licenses

Cisco ISE licensing offers two options to manage your licenses:

- Smart Licensing—Monitor ISE software licenses and endpoint license consumption easily and efficiently with a single token registration. The licenses that you have purchased are maintained in a centralized database called the Cisco Smart Software Manager (CSSM). For more information about Smart Licensing, see Cisco ISE Smart Licensing, on page 637.

- Traditional Licensing—Purchase and import individual licenses based on your needs and manage the application features and access, such as the number of concurrent endpoints that can use Cisco ISE network resources. For more information about Traditional Licensing, see Manage Traditional License Files, on page 128.

To maximize economy for customers, licensing in Cisco ISE is supplied in different packages as Base, Plus, Apex, and Device Administration for both Traditional and Smart Licensing options. For more information about the Traditional Cisco licensing model, see Cisco ISE Licensing Model, on page 128.

Once you have installed or upgraded your ISE box, Traditional Licensing is in use by default, and all license components are activated for a 90-day trial period. Once you switch to Smart Licensing, and before you register your token, this evaluation period remains active for the Smart Licensing, and the evaluation period includes all ISE licenses as part of that evaluation period. During the evaluation period, consumption is not reported to the CSSM.

You should update your installed licenses (for Traditional licensing) or license agreements (for Smart licensing) if:

- The trial period ends and you have not yet installed or registered your license.
- Your license has expired.
- If endpoint consumption exceeds your licensing agreement.
ISE will notify you of license expiration or consumption problems 90, 60 and 30 days in advance. Once the system is no longer compliant, the administrator will no longer be able to edit or configure Plus and Apex features. You can view and track licensing details from the **License Warning** icon at the top of the screen.

When upgrading from one licensing package to another more complex package, Cisco ISE will continue to offer all features that were available in the earlier package prior to upgrade and you will not need to re-configure any settings that you had already configured.

---

### Manage Traditional License Files

To continue to use Cisco ISE services after the 90-day Evaluation license expires, and to support more than 100 concurrent endpoints on the network, you must obtain and register Base licenses for the number of concurrent users on your system. If you require additional functionality, you will need Plus and/or Apex licenses to enable that functionality.

Licenses are uploaded to the Primary Administration Node (PAN) and propagated to the other Cisco ISE nodes in the cluster. Licenses are centrally managed by the Administration node, the other nodes do not require separate licenses. If you have two Administration nodes deployed in a high-availability pair, you must ensure that each of them have the same license capabilities. Generate licenses with both UDIs and then add the licenses while each node is in a standalone or primary state.

After you install the Cisco ISE software and initially configure the appliance as the PAN, you must obtain a license for Cisco ISE and then register that license. You register all licenses to the PAN via the Primary and Secondary Administration Node hardware UDI. The PAN then centrally manages all the licenses that are registered for your deployment.

---

**Note**

When a node is deregistered from the PAN, it becomes a standalone node and its license is reset to Evaluation.

This section explains how to register, re-host, renew, migrate, upgrade, and remove Traditional ISE licenses.

---

### Cisco ISE Licensing Model

Cisco ISE licensing model allows you to purchase licenses based on your enterprise's needs. When using Traditional Licensing, you import all individual licenses and continue to manage them individually from ISE. When using Smart Licensing, you manage a centralized Cisco account, which contains all information about the different endpoint licenses you have purchased.

Valid license options include:

- ISE Base only
- ISE Base and Plus
- ISE Base and Apex
- ISE Base and Device Administration
• ISE Base, Plus, Apex, and Device Administration
• ISE Base, Plus, Apex and AnyConnect Apex

The number of Plus license sessions can be up to the number of Base license sessions on the deployment. The same stands for Apex license sessions. Apex and Plus licenses can be installed independently without any restriction on the number of Apex versus Plus licenses. Cisco ISE licenses are based on the number of concurrent endpoints with active network connections whereas AnyConnect Apex licenses are on a per user basis. AnyConnect Apex license count can exceed Cisco ISE Base license count.

Note
The services contained within the Plus license, most notably profiling, are frequently used across the entire deployment. When you add Plus licenses to the deployment, we recommend that the Plus license count be equal to the Base license count. However, you might have a situation where the Plus license services might not be needed across the entire deployment, which is why Cisco ISE allows the Plus license count to be less than the Base license count.

Cisco recommends installing (for Traditional Licensing), or purchasing (for Smart Licensing) Base, Plus, and Apex licenses at the same time.

• Base licenses are required to use the services enabled by Plus and/or Apex licenses. However, you do not need a Plus license in order to have an Apex license or vice versa, since there is no overlap in their functionality.

• When you install a Base or Mobility Upgrade license, Cisco ISE continues to use the default Evaluation license as a separate license for the remainder of its duration.

• When you install a Mobility Upgrade license, Cisco ISE enables all Wired, Wireless, and VPN services.

• A Base or Mobility license is required to install the Device Administration license.

• You cannot upgrade the Evaluation license to a Plus license without first installing the Base license.

<table>
<thead>
<tr>
<th>Table 5: Cisco ISE License Packages</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISE License Packages</td>
</tr>
<tr>
<td>----------------------</td>
</tr>
<tr>
<td>Base</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

Passive identity services available as part of the upgrade from ISE-PIC to a Base license include limited pxGrid features available to Cisco subscribers only.
<table>
<thead>
<tr>
<th>License</th>
<th>Subscription Duration</th>
<th>Services</th>
<th>Notes</th>
</tr>
</thead>
</table>
| **Plus**       | Subscription (1, 3, or 5 years) | • Bring Your Own Device (BYOD) — when consuming either a built-in or an external certificate authority  
• MSE integration for location services  
• Profiling and Feed Services  
• Adaptive Network Control (ANC)  
• Cisco pxGrid | Does not include Base services; a Base license is required to install the Plus license.  
When onboarding an endpoint with the BYOD flow, the Plus services are consumed on the active session even when related BYOD attributes are not in use. |
| **Apex**       | Subscription (1, 3, or 5 years) | • Third Party Mobile Device Management (MDM) integration  
• Posture Compliance  
• TC NAC | Does not include Base services; a Base license is required to install the Apex license.  
**Note** When you use Cisco AnyConnect as a unified posture agent across wired, wireless, and VPN deployments, you need Cisco AnyConnect Apex user licenses in addition to Cisco ISE Apex licenses. |
| **Mobility**   | Subscription (1, 3, or 5 years) | Combination of Base, Plus, and Apex for wireless and VPN endpoints | Cannot coexist on a Cisco Administration node with Base, Plus, and/or Apex licenses. |
| **Mobility Upgrade** | Subscription (1, 3, or 5 years) | Provides wired support to Mobility license | You can only install a Mobility Upgrade license on top of an existing Mobility license. |
| **Device Administration** | Perpetual | TACACS+ | A Base or Mobility license is required to install the Device Administration license.  
Only one license is required per deployment (regardless of multiple nodes). |
| **ISE-PIC**    | Perpetual | Passive identity services | One license per node. Each license supports up to 3,000 parallel sessions. |
ISE-PIC upgrade  Perpetual  This license allows these options:
  • Enable additional (up to 300,000) parallel sessions.
  • Upgrade to full ISE instance
  One license per node. Each license supports up to 300,000 parallel sessions.
  After installing this license, the upgraded node can join an existing ISE deployment or alternatively, base licenses can be installed on the node to function as the PAN.
  Passive identity services available as part of the upgrade to a Base license include limited pxGrid features available to Cisco subscribers only.

Evaluation  Temporary (90 days)  Full Cisco ISE functionality is provided for 100 endpoints.  All Cisco ISE appliances are supplied with an Evaluation license.

### Traditional License Consumption

You purchase licenses for the number of concurrent users on the system with Traditional Licensing. A Cisco ISE user consumes a license during an active session (always a Base; and a Plus and an Apex license, if you use the functionality covered by these licenses). Once the session ends, the license is released for reuse by other users.

---

**Restriction**

Cisco ISE license architecture consumption logic relies on authorization policy constructs. Cisco ISE uses the dictionaries and attributes within authorization rules to determine the license to use.

The Cisco ISE license is counted as follows:

- A Base license is consumed for every active session. The same endpoint also consumes Plus and Apex licenses depending on the features that it is using.

  **Note** TACACS+ sessions do not consume a base license, but RADIUS sessions consume a base license.

- The endpoint consumes the Base license before it consumes a Plus and Apex license.
- The endpoint consumes the Plus license before it consumes an Apex license.
- One Plus license is consumed per endpoint for any assortment of the license's features. Likewise, one Apex license is consumed per endpoint for any assortment of its features.
- Licenses are counted against concurrent, active sessions.
- Licenses are released for all features when the endpoint's session ends.
• pxGrid is used to share context collected by ISE with other products. A Plus license is required to enable pxGrid functionality. There is no session count decrement when context for session is shared. However, to use pxGrid, the number of Plus sessions licensed must be equal to the number of Base sessions licensed. For more information, see Cisco ISE Licenses and Services section in Cisco Identity Services Engine Ordering Guide.

• One AnyConnect Apex user license is consumed by each user who uses AnyConnect regardless of the number of devices that the user owns and whether or not the user has an active connection to the network.

• You can enable the TACACS+ service by adding a Device Administration license on top of an existing Base or Mobility license. This feature does not consume licenses.

To avoid service disruption, Cisco ISE continues to provide services to endpoints that exceed license entitlement. Cisco ISE instead relies on RADIUS accounting functions to track concurrent endpoints on the network and generates an alarm when the endpoint count of the previous day exceeded the amount of licenses. You can view license consumption clearly from the License Usage area in the Licensing screen, where licenses that are consumed beyond the permitted quantity appear in red in the line graph.

In addition, you can view and track detailed information per license package from the License Warning icon at the top of the screen.

View License Consumption

You can view your system's current license consumption from the Licensing dashboard at: Administration > System > Licensing. Consumption is portrayed as in the following image:

Figure 4: Traditional License Consumption

The License Consumption graph, in the License Usage area, is updated every 30 minutes. This window also displays the type of licenses purchased, the total number of concurrent users permitted on the system, and the expiry date of subscription services.

If you want to see your system's license consumption over multiple weeks, click Usage Over Time. Each bar in the graph shows the maximum number of licenses used during a period of one week.
Unregistered License Consumption

Problem
License consumption relies on the attributes used in the authorization policy with which the endpoint is matched.

Consider you only have a Base license registered on your system (you deleted the 90-day Evaluation license). You will be able to see and configure the corresponding Base menu items and features.

If you configure (mis-configure) an authorization policy to use a feature (for example: Session:PostureStatus) that requires an Apex license, and if an endpoint matches this authorization policy then:

- The endpoint will consume an Apex license, despite the fact that an Apex license has not been registered on the system.
- Notifications to this effect will appear whenever you log in.
- Cisco ISE will give notifications and alarms "Exceeded license usage than allowed" (technically, this is to be expected as there are no registered Apex licenses on the system, but an endpoint is never-the-less consuming one).

Possible Causes
Due to authorization policy mis-configuration, the Licensing dashboard can show that Cisco ISE is consuming a license you have not purchased and registered. Before you purchase Plus and Apex licenses, the ISE user interface does not display the functionality covered by those licenses. However, once you have purchased these licenses, the user interface continues to display their functionality even after the license has expired or exceeded its endpoint consumption. Thus, you are able to configure them even if you do not have a valid license for them.

Solution
Choose Policy > Policy Sets, identify the authorization rule that is using the feature(s) for which you do not have a registered license, and reconfigure that rule.

Manage License Files
This section explains how to register, re-host, renew, migrate, upgrade, and remove ISE licenses:

- Register Licenses, on page 133
- Re-Host Licenses, on page 134
- Renew Licenses, on page 134
- Migrate and Upgrade Licenses, on page 134
- Remove Licenses, on page 135

Register Licenses

Before you begin
Consult your Cisco partner/account team about the types of licenses and number of concurrent users you require for your installation, together with the various packages you can purchase to maximize economy.
**Step 1**
From the ordering system (Cisco Commerce Workspace - CCW) on Cisco's website [www.cisco.com](http://www.cisco.com), order the required licenses.

After about an hour, an email confirmation containing the Product Authorization Key (PAK) is sent.

**Step 2**
From the Cisco ISE Administration portal, choose **Administration > System > Licensing**. Make a note of the node information in the **Licensing Details** section: Product Identifier (PID), Version Identifier (VID), and Serial Number (SN).

**Step 3**
Go to [www.cisco.com/go/licensing](http://www.cisco.com/go/licensing), and where prompted, enter the PAK of the license you received, the node information, and some details about your company.

After one day, Cisco sends you the license file.

**Step 4**
Save this license file to a known location on your system.

**Step 5**
From the Cisco ISE Administration portal, choose **Administration > System > Licensing**. In the **License Files** section, click the **Import License** button.

**Step 6**
Click **Choose File** and select the license file you previously stored on your system.

**Step 7**
Click **Import**.

The new license is now installed on your system.

**What to do next**
Choose the licensing dashboard, **Administration > System > Licensing**, and verify that the newly-entered license appears with the correct details.

---

**Re-Host Licenses**

Re-hosting means moving a license from one Cisco ISE node to another. From the licensing portal, you select the PAK of the license you want to move and follow the instructions for re-hosting. After one day, you are sent an email with a new PAK. You then register this new PAK for the new node, and remove the old license from the original Cisco ISE node.

**Renew Licenses**

Subscription licenses, such as Plus and Apex licenses, are issued for 1, 3 or 5 years. Cisco ISE sends an alarm when licenses are near their expiration date and again when the licenses expire.

Licenses must be renewed after they expire. This process is carried out by your Cisco partner or account team only.

**Migrate and Upgrade Licenses**

Cisco licensing policy supports migration from previous Cisco ISE versions, upgrading from wireless and VPN only to include wired deployments, and adding concurrent users and functionality. You can also purchase bundles of licenses to minimize your ongoing expenses. These scenarios are all covered in the [licensing site](http://licensing-site.com), or for more information contact your Cisco partner/account team.

**Note**
If you have migrated from Cisco ISE version 1.2, your Advanced license covers all the features in both Plus and Apex licenses.
After upgrading from Cisco ISE version 1.3 or 1.4, the system will show the default Evaluation license only if it existed on the system prior to upgrade.

Note
Mobility/Mobility Upgrade license is always displayed as Base/Plus/Apex in the user interface with its corresponding number of end points.

If your Cisco ISE node needs to support:
- A larger number of concurrent users than the number for which you have licenses
- Wired (LAN) access, and your system has only the Mobility license

You will need to upgrade your license(s) for that node. This process is carried out by your Cisco partner or account team only.

Remove Licenses

Before you begin
Keep the following in mind before attempting to remove a license:
- If you have installed a Mobility Upgrade license after a Mobility license, you must remove the Mobility Upgrade license before you can remove the underlying Mobility license.
- If you install a combined license, all related installations in the Base, Plus, and Apex packages are also removed.

Step 1 Choose Administration > System > Licensing
Step 2 In the License Files section, click the check next to the relevant file name, and click Delete License.
Step 3 Click OK.
Remove Licenses
Manage Certificates

- Certificate Management in Cisco ISE, on page 137
- Cisco ISE CA Service, on page 164
- OCSP Services, on page 190

Certificate Management in Cisco ISE

A certificate is an electronic document that identifies an individual, a server, a company, or other entity and associates that entity with a public key. A self-signed certificate is signed by its own creator. Certificates can be self-signed or digitally signed by an external Certificate Authority (CA). A CA-signed digital certificate is considered industry standard and more secure.

Certificates are used in a network to provide secure access. Cisco ISE uses certificates for internode communication, and for communicating with external servers such as the syslog server, feed server, and all the end-user portals (guest, sponsor, and personal devices portals). Certificates identify a Cisco ISE node to an endpoint and secures the communication between that endpoint and the Cisco ISE node.

You can use the Admin portal to manage certificates for all the nodes in your deployment.

Certificates Enable Cisco ISE to Provide Secure Access

The Cisco Identity Services Engine (ISE) relies on public key infrastructure (PKI) to provide secure communication with both endpoints and administrators, as well as between Cisco ISE nodes in a multinode deployment. PKI relies on X.509 digital certificates to transfer public keys for encryption and decryption of messages, and to verify the authenticity of other certificates representing users and devices. Cisco ISE provides the Admin Portal to manage the following two categories of X.509 certificates:

- System certificates—These are server certificates that identify a Cisco ISE node to client applications. Every Cisco ISE node has its own system certificates, each of which are stored on the node along with the corresponding private key.

- Trusted certificates—These are certificate authority (CA) certificates used to establish trust for the public keys received from users and devices. The Trusted Certificates Store also contains certificates that are distributed by the Simple Certificate Enrollment Protocol (SCEP), which enables registration of mobile devices into the enterprise network. Certificates in the Trusted Certificates Store are managed on the Primary Administration Node (PAN), and are automatically replicated to all other nodes in an Cisco ISE deployment.
Certificate Usage

In a distributed deployment, you must import the certificate only in to the certificate trust list (CTL) of the PAN. The certificate gets replicated to the secondary nodes.

In general, to ensure certificate authentication in Cisco ISE is not impacted by minor differences in certificate-driven verification functions, use lower case hostnames for all Cisco ISE nodes deployed in a network.

Certificate Usage

When you add or import a certificate in to Cisco ISE, you should specify the purpose for which the certificate is to be used:

- Admin: For internode communication and authenticating the Admin portal
- EAP: For TLS-based EAP authentication
- RADIUS DTLS: For RADIUS DTLS server authentication
- Portal: For communicating with all Cisco ISE end-user portals
- xGrid: For communicating with the pxGrid controller

You can associate different certificates from each node for communicating with the Admin portal (Admin), the pxGrid controller (xGrid), and for TLS-based EAP authentication (EAP). However, you can associate only one certificate from each node for each of these purposes.

With multiple Policy Service nodes (PSNs) in a deployment that can service a web portal request, Cisco ISE needs a unique identifier to identify the certificate that has to be used for portal communication. When you add or import certificates that are designated for portal use, you must define a certificate group tag and associate it with the corresponding certificate on each node in your deployment. You must associate this certificate group tag to the corresponding end-user portals (guest, sponsor, and personal devices portals). This certificate group tag is the unique identifier that helps Cisco ISE identify the certificate that has to be used when communicating with each of these portals. You can designate one certificate from each node for each of the portals.
EAP-TLS client certificate should have KeyUsage=Key Agreement and ExtendedKeyUsage=Client Authentication for the following ciphers:

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-SHA384

EAP-TLS client certificate should have KeyUsage=Key Encipherment and ExtendedKeyUsage=Client Authentication for the following ciphers:

- AES256-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES256-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-SHA
- ECDHE-RSA-AES128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- RC4-SHA
- RC4-MD5

**Certificate Matching in Cisco ISE**

When you set up Cisco ISE nodes in a deployment, those two nodes communicate with each other. The system checks the FQDN of each ISE node to ensure they match (for example ise1.cisco.com and ise2.cisco.com or if you use wild card certificates then *.cisco.com). In addition, when an external machine presents a certificate
to an ISE server, the external certificate that is presented for authentication is checked (or matched) against the certificate in the ISE server. If the two certificates match, the authentication succeeds.

For matching, if matching is performed between the nodes (if there are two) and between the and pxGrid.

Cisco ISE checks for a matching subject name as follows:

1. Cisco ISE looks at the subject alternative name (SAN) extension of the certificate. If the SAN contains one or more DNS names, then one of the DNS names must match the FQDN of the Cisco ISE node. If a wildcard certificate is used, then the wildcard domain name must match the domain in the Cisco ISE node’s FQDN.

2. If there are no DNS names in the SAN, or if the SAN is missing entirely, then the Common Name (CN) in the Subject field of the certificate or the wildcard domain in the Subject field of the certificate must match the FQDN of the node.

3. If no match is found, the certificate is rejected.

---

**Validity of X.509 Certificates**

X.509 certificates are only valid until a specific date. When a system certificate expires, the Cisco ISE functionality that depends on the certificate is impacted. Cisco ISE notifies you about the pending expiration of a system certificate when the expiration date is within 90 days. This notification appears in several ways:

- Colored expiration status icons appear in the System Certificates page.
- Expiration messages appear in the Cisco ISE System Diagnostic report.
- Expiration alarms are generated at 90 days, 60 days, and every day in the final 30 days before expiration.

If the expiring certificate is a self-signed certificate, you can extend its expiration date by editing the certificate. For a CA-signed certificate, you must allow sufficient time to acquire replacement certificate from your CA.

**Enable PKI in Cisco ISE**

Public Key Infrastructure (PKI) is a cryptographic technique that enables secure communication and verifies the identity of a user using digital signatures.

---

**Step 1**

Establish system certificates on each deployment node for TLS-enabled authentication protocols such as EAP-TLS, for authenticating the Admin portal, for browser and REST clients to access the Cisco ISE web portals, and for the pxGrid controller.

By default, a Cisco ISE node is preinstalled with a self-signed certificate that is used for EAP authentication, Admin portal, portals, and pxGrid controller. In a typical enterprise environment, this certificate is replaced with server certificates that are signed by a trusted CA.
Step 2

Populate the Trusted Certificates Store with the CA certificates that are necessary to establish trust with the user as well as device certificates that will be presented to Cisco ISE.

If a certificate chain consists of a root CA certificate plus one or more intermediate CA certificates, to validate the authenticity of a user or device certificate, you must import the entire chain into the Trusted Certificates Store.

For inter-node communication, you must populate the Trusted Certificates Store with the trust certificate(s) needed to validate the Admin system certificate belonging to each node in the Cisco ISE deployment. If you want to use the default self-signed certificate for internode communication, then you must export this certificate from the System Certificates page of each Cisco ISE node and import it into the Trusted Certificates Store. If you replace the self-signed certificates with CA-signed certificates, it is only necessary to populate the Trusted Certificates Store with the appropriate root CA and intermediate CA certificates. Be aware that you cannot register a node in a Cisco ISE deployment until you complete this step.

If you use self-signed certificates to secure communication between a client and PSN in a deployment, when BYOD users move from one location to another, EAP-TLS user authentication fails. For such authentication requests that have to be serviced between a few PSNs, you must secure communication between the client and PSN with an externally-signed CA certificate or use wildcard certificates signed by an external CA.

If you intend to get a publicly-signed certificate or if the Cisco ISE deployment is to be operated in FIPS mode, you must ensure that all system and trusted certificates are FIPS-compliant. This means that each certificate must have a minimum key size of 2048 bytes, and use SHA-1 or SHA-256 encryption.

Note: After you obtain a backup from a standalone Cisco ISE node or the PAN, if you change the certificate configuration on one or more nodes in your deployment, you must obtain another backup to restore data. Otherwise, if you try to restore data using the older backup, communication between the nodes might fail.

---

Wildcard Certificates

A wildcard certificate uses a wildcard notation (an asterisk and period before the domain name) and allows the certificate to be shared across multiple hosts in an organization. For example, the CN value for the Certificate Subject would be some generic hostname such as aaa.ise.local and the SAN field would include the same generic hostname and the wildcard notation such as DNS.1=aaa.ise.local and DNS.2=*.ise.local.

If you configure a wildcard certificate to use *.ise.local, you can use the same certificate to secure any other host whose DNS name ends with “.ise.local,” such as:

- aaa.ise.local
- psn.ise.local
- mydevices.ise.local
- sponsor.ise.local

Wildcard certificates secure communication in the same way as a regular certificate, and requests are processed using the same validation methods.

The following figure shows an example of a wildcard certificate that is used to secure a web site.
Wildcard Certificate Support in Cisco ISE

Cisco ISE supports wildcard certificates. In earlier releases, Cisco ISE verified any certificate enabled for HTTPS to ensure the CN field matches the Fully Qualified Domain Name (FQDN) of the host exactly. If the fields did not match, the certificate could not be used for HTTPS communication.

In earlier releases, Cisco ISE used that CN value to replace the variable in the url-redirect A-V pair string. For all Centralized Web Authentication (CWA), onboarding, posture redirection, and so on, the CN value was used.

Cisco ISE uses the hostname of the ISE node as the CN.

Wildcard Certificates for HTTPS and EAP Communication

You can use wildcard server certificates in Cisco ISE for Admin (web-based service) and EAP protocols that use SSL/TLS tunneling. With the use of wildcard certificates, you no longer have to generate a unique certificate for each Cisco ISE node. Also, you no longer have to populate the SAN field with multiple FQDN values to prevent certificate warnings. Using an asterisk (*) in the SAN field allows you to share a single certificate across multiple nodes in a deployment and helps prevent certificate name mismatch warnings. However, use of wildcard certificates is considered less secure than assigning a unique server certificate for each Cisco ISE node.

When assigning public wildcard certificates to the guest portal and importing sub-CA with root-CA certificates, the certificate chain is not sent until the ISE services are restarted.
If you use wildcard certificates, we strongly recommend that you partition your domain space for greater security. For example, instead of *.example.com, you can partition it as *.amer.example.com. If you do not partition your domain, it can lead to serious security issues.

Wildcard certificate uses an asterisk (*) and a period before the domain name. For example, the CN value for a certificate’s Subject Name would be a generic host name such as aaa.ise.local and the SAN field would have the wildcard character such as *.ise.local. Cisco ISE supports wildcard certifications in which the wildcard character (*) is the left most character in the presented identifier. For example, *.example.com or *.ind.example.com. Cisco ISE does not support certificates in which the presented identifier contains additional characters along with the wildcard character. For example, abc*.example.com or a*b.example.com or *abc.example.com.

**Fully Qualified Domain Name in URL Redirection**

When Cisco ISE builds an authorization profile redirect (for central web authentication, device registration web authentication, native supplicant provisioning, mobile device management, and client provisioning and posture services), the resulting cisco-av-pair includes a string similar to the following:

```
url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa
```

When processing this request, Cisco ISE substitutes actual values for some keywords in this string. For eth0 interface, Cisco ISE replaces the IP in the URL with the FQDN of the Cisco ISE node. For non-eth0 interfaces, Cisco ISE uses the IP address in the URL. You can assign a host alias(name) for interfaces eth1 through eth3, which Cisco ISE can then substitute in place of IP address during URL redirection.

To do this, you can use the `ip host` command in the configuration mode from the Cisco ISE CLI ISE /admin(config)# prompt:

```
ip host IP_address host-alias FQDN-string
```

where IP_address is the IP address of the network interface (eth1 or eth2 or eth3) and host-alias is the name that you assign to the network interface. FQDN-string is the fully qualified domain name of the network interface. Using this command, you can assign a host-alias or an FQDN-string or both to a network interface.

Here is an example using the `ip host` command: `ip host a.b.c.d sales.sales.amerxyz.com`

After you assign a host alias to the non-eth0 interface, you must restart the application services on Cisco ISE using the `application start ise` command.

Use the no form of this command to remove the association of the host alias with the network interface.

```
no ip host IP_address host-alias FQDN-string
```

Use the `show running-config` command to view the host alias definitions.

If you provide the FQDN-string, Cisco ISE replaces the IP address in the URL with the FQDN. If you provide only the host alias, Cisco ISE combines the host alias with the configured IP domain name to form a complete FQDN, and replaces the IP address in the URL with the FQDN. If you do not map a network interface to a host alias, then Cisco ISE uses the IP address of the network interface in the URL.

When you make use of non-eth0 interfaces for client provisioning or native supplicant or guest flows, you have to make sure that the IP address or host alias for non-eth0 interfaces should be configured appropriately in the Policy Service node certificate's SAN fields.
Advantages of Using Wildcard Certificates

• Cost savings. Certificates signed by a third party Certificate Authority is expensive, especially as the number of servers increase. Wildcard certificates may be used on multiple nodes in the Cisco ISE deployment.

• Operational efficiency. Wildcard certificates allow all Policy Service Node (PSN) EAP and web services to share the same certificate. In addition to significant cost savings, certificate administration is also simplified by creating the certificate once and applying it on all the PSNs.

• Reduced authentication errors. Wildcard certificates address issues seen with Apple iOS devices where the client stores trusted certificates within the profile, and does not follow the iOS keychain where the signing root is trusted. When an iOS client first communicates with a PSN, it does not explicitly trust the PSN certificate, even though a trusted Certificate Authority has signed the certificate. Using a wildcard certificate, the certificate will be the same across all PSNs, so the user only has to accept the certificate once and successive authentications to different PSNs proceed without error or prompting.

• Simplified supplicant configuration. For example, Microsoft Windows supplicant with PEAP-MSCHAPv2 and server certificate trust enabled requires that you specify each of the server certificate to trust, or the user may be prompted to trust each PSN certificate when the client connects using a different PSN. With wildcard certificates, a single server certificate can be trusted rather than individual certificates from each PSN.

• Wildcard certificates result in an improved user experience with less prompting and more seamless connectivity.

Disadvantages of Using Wildcard Certificates

The following are some of the security considerations related to wildcard certificates:

• Loss of auditability and nonrepudiation

• Increased exposure of the private key

• Not common or understood by administrators

Wildcard certificates are considered less secure than a unique server certificate per ISE node. But, cost and other operational factors outweigh the security risk.

Security devices such as ASA also support wildcard certificates.

You must be careful when deploying wildcard certificates. For example, if you create a certificate with *.company.local and an attacker is able to recover the private key, that attacker can spoof any server in the company.local domain. Therefore, it is considered a best practice to partition the domain space to avoid this type of compromise.

To address this possible issue and to limit the scope of use, wildcard certificates may also be used to secure a specific subdomain of your organization. Add an asterisk (*) in the subdomain area of the common name where you want to specify the wildcard.

For example, if you configure a wildcard certificate for *.ise.company.local, that certificate may be used to secure any host whose DNS name ends in “.ise.company.local”, such as:

• psn.ise.company.local

• mydevices.ise.company.local
• sponsor.ise.company.local

**Wildcard Certificate Compatibility**

Wildcard certificates are usually created with the wildcard listed as the Common Name (CN) of the Certificate Subject. Cisco ISE supports this type of construction. However, not all endpoint supplicants support the wildcard character in the Certificate Subject.

All Microsoft native supplicants tested (including Windows Mobile) do not support wildcard character in the Certificate Subject.

You can use another supplicant, such as Cisco AnyConnect Network Access Manager (NAM) that might allow the use of wildcard character in the Subject field.

You can also use special wildcard certificates such as DigiCert's Wildcard Plus that is designed to work with incompatible devices by including specific subdomains in the Subject Alternative Name of the certificate.

Although the Microsoft supplicant limitation appears to be a deterrent to using wildcard certificates, there are alternative ways to create the wildcard certificate that allow it to work with all devices tested for secure access, including the Microsoft native supplicants.

To do this, instead of using the wildcard character in the Subject, you must use the wildcard character in the Subject Alternative Name (SAN) field instead. The SAN field maintains an extension designed for checking the domain name (DNS name). See RFCs 6125 and 2128 for more information.

**Certificate Hierarchy**

From the Admin portal, you can view the certificate hierarchy or the certificate trust chain of all endpoint, system, and trusted certificates. The certificate hierarchy includes the certificate, all intermediate Certificate Authority (CA) certificates, and the root certificate. For example, when you choose to view a system certificate from the Admin portal, by default, the details of the corresponding system certificate appear. The certificate hierarchy appears at the top of the certificate. Click any of the certificates in the hierarchy to view its details. The self-signed certificate does not have any hierarchy or trust chain.

In the certificate listing pages, you will see one of the following icons in the Status column:

- Green icon—Indicates a valid certificate (valid trust chain)
- Red icon—Indicates an error (for example, trust certificate missing or expired)
- Yellow icon—Warns that a certificate is about to expire and prompts renewal

**System Certificates**

Cisco ISE system certificates are server certificates that identify a Cisco ISE node to other nodes in the deployment and to client applications. System certificates are:

- Used for inter-node communication in a Cisco ISE deployment. Choose the Admin option in the Usage field for these certificates.
- Used by browser and REST clients who connect to Cisco ISE web portals. Choose the Portal option in the Usage field for these certificates.
- Used to form the outer TLS tunnel with PEAP and EAP-FAST. Choose the EAP option in the Usage field for mutual authentication with EAP-TLS, PEAP, and EAP-FAST.
• Used for RADIUS DTLS server authentication.

• Used to communicate with the SAML Identity Provider (IdP). Choose the SAML option in the Usage field for this certificate. If you choose the SAML option, you cannot use this certificate for any other service.

• Used to communicate with the pxGrid controller. Choose the pxGrid option in the Usage field for these certificates.

You must install valid system certificates on each node in your Cisco ISE deployment. By default, two self-signed certificates and one signed by the internal Cisco ISE CA are created on a Cisco ISE node during installation time:

• A self-signed server certificate designated for EAP, Admin, Portal, and RADIUS DTLS (it has a key size of 2048 and is valid for one year)

• A self-signed SAML server certificate that can be used to secure communication with a SAML IdP (it has a key size of 2048 and is valid for one year)

• An internal Cisco ISE CA-signed server certificate that can be used to secure communication with pxGrid clients (it has a key size of 4096 and is valid for one year).

When you set up a deployment and register a secondary node, the certificate designated for pxGrid controller is automatically replaced with a certificate that is signed by the primary node's CA. Thus, all pxGrid certificates become part of the same PKI trust hierarchy.

---

**Note**

When you export a wildcard system certificate to be imported in to the other nodes (for inter-node communication), ensure that you export the certificate and private key, and specify an encryption password. During import, you will need the certificate, private key, and encryption password.

Cisco recommends that you replace the self-signed certificate with a CA-signed certificates for greater security. To obtain a CA-signed certificate, you must:

1. Create a certificate signing request (CSR)
2. Submit it to a Certificate Authority (CA)
3. Obtain the signed certificate
4. Import the relevant root and intermediate CA certificates in to the Trusted Certificates Store
5. Bind the signed certificate with the CSR

---

### ISE Community Resource

How To: Implement ISE Server-Side Certificates
Certificate Renewal on Cisco Identity Services Engine Configuration Guide

---

**View System Certificates**

The System Certificate page lists all the system certificates added to Cisco ISE.
Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1  Choose Administration > System > Certificates > System Certificates.

The System Certificates page appears and provides the following information for the local certificates:

- Friendly Name—Name of the certificate.
- Used By—Service for which this certificate is used.
- Portal group tag—Applicable only for certificates that are designated for portal use. Specifies which certificate has to be used for the portals.
- Issued To—Common Name of the certificate subject.
- Issued By—Common Name of the certificate issuer
- Valid From—Date on which the certificate was created, also known as the Not Before certificate attribute.
- Expiration Date—Expiration date of the certificate, also known as the Not After certificate attribute. Indicates when the certificate expires. There are five categories along with an associated icon that appear here:
  - Expiring in more than 90 days (green icon)
  - Expiring in 90 days or less (blue icon)
  - Expiring in 60 days or less (yellow icon)
  - Expiring in 30 days or less (orange icon)
  - Expired (red icon)

Step 2  Select a certificate and choose View to display the certificate details.

Import a System Certificate

You can import a system certificate for any Cisco ISE node from the Admin portal.

Before you begin

- Ensure that you have the system certificate and the private key file on the system that is running the client browser.
- If the system certificate that you import is signed by an external CA, import the relevant root CA and intermediate CA certificates in to the Trusted Certificates Store (Administration > System > Certificates > Trusted Certificates).
- Cisco ISE does not support certificates that are signed with a hash algorithm greater than SHA-256. Hence, you must not import a server certificate that is signed with a hash algorithm greater than SHA-256.
- If the system certificate that you import contains the basic constraints extension with the CA flag set to true, ensure that the key usage extension is present, and the keyEncipherment bit or the keyAgreement bit or both are set.
To perform the following task, you must be a Super Admin or System Admin.

**Step 1** Choose Administration > System > Certificates > System Certificates.

**Step 2** Click Import.
The Import Server Certificate screen opens.

**Step 3** Enter the values for the certificate that you are going to import.

**Step 4** Click Submit.

---

### Generate a Self-Signed Certificate

You can add a new local certificate by generating a self-signed certificate. Cisco recommends that you only employ self-signed certificates for your internal testing and evaluation needs. If you are planning to deploy Cisco ISE in a production environment, be sure to use CA-signed certificates whenever possible to ensure more uniform acceptance around a production network.

**Note**

If you are using a self-signed certificate and you must change the hostname of your Cisco ISE node, you must log in to the Admin portal of the Cisco ISE node, delete the self-signed certificate that has the old hostname, and generate a new self-signed certificate. Otherwise, Cisco ISE will continue to use the self-signed certificate with the old hostname.

---

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

**Step 1** Choose Administration > System > Certificates > System Certificates.

To generate a self-signed certificate from a secondary node, choose Administration > System > Server Certificate.

**Step 2** Click Generate Self Signed Certificate and enter the details in the Generate Self Signed Certificate page.

**Step 3** Check the Allow Wildcard Certificates checkbox if you want to generate a self-signed wildcard certificate (a certificate that contains an asterisk (*) in any Common Name in the Subject and/or the DNS name in the Subject Alternative Name. For example, DNS name assigned to the SAN can be *.amer.cisco.com.

**Step 4** Check the checkboxes in the Usage area based on the service for which you want to use this certificate.

**Step 5** Click Submit to generate the certificate.

To restart the secondary nodes, from the CLI, enter the following commands in the given order:

a) `application stop ise`

b) `application start ise`
Edit a System Certificate

You can use this page to edit a system certificate and to renew a self-signed certificate. When you edit a wildcard certificate, the changes are replicated to all the nodes in the deployment. If you delete a wildcard certificate, that wildcard certificate is removed from all the nodes in the deployment.

Before you begin
To perform the following task, you must be a Super Admin or System Admin.

Step 1
Choose Administration > System > Certificates > System Certificates.

Step 2
Check the check box next to the certificate that you want to edit, and click Edit.

Step 3
To renew a self-signed certificate, check the Renewal Period check box and enter the Expiration TTL (Time to Live) in days, weeks, months, or years.

Step 4
Click Save to save your changes.

If the Admin check box is checked, then the application server on the Cisco ISE node will be restarted. In addition, if the Cisco ISE node is the PAN in a deployment, then the application server on all other nodes in the deployment will also be restarted. The system restarts one node at a time, after the Primary Administration Node (PAN) restart has completed.

Note
Using Chrome 65 and above to launch ISE can cause BYOD portal or Guest portal to fail to launch in the browser even though URL is redirected successfully. This is because of a new security feature introduced by Google that requires all certificates to have a Subject Alternative Name field. All ISE releases until ISE 2.4 don’t fill the Subject Alternative Name field.

To launch with Chrome 65 and above, follow the steps below:
1. Generate a new self-signed certificate from ISE GUI by filling the Subject Alternative Name field. Both DNS and IP Address must be filled.
2. ISE services will now restart.
3. Redirect the portal in Chrome browser.
4. From browser View Certificate>Details>Copy the certificate by selecting base-64 encoded.
5. Install the certificate in Trusted path.
6. Close the Chrome browser and try to redirect the portal.

Delete System Certificate

You can delete system certificates that you no longer use.

Even though you can delete multiple certificates from the System Certificates store at a time, you must have at least one certificate that can be used for Admin and EAP authentication. Also, you cannot delete any certificate that is in use for Admin, EAP Authentication, Portals, or pxGrid controller. However, you can delete the pxGrid certificate when the service is disabled.

If you choose to delete a wildcard certificate, the certificate is removed from all the nodes in the deployment.
Export a System Certificate

You can export a selected system certificate or a certificate and its associated private key. If you export a certificate and its private key for backup purposes, you can reimport them later if needed.

**Before you begin**
To perform the following task, you must be a Super Admin or System Admin.

---

**Step 1** Choose Administration > System > Certificates > System Certificates.

**Step 2** Check the checkboxes next to the certificates that you want to delete, and click **Delete**.

A warning message appears.

**Step 3** Click **Yes** to delete the certificate.

---

Export a System Certificate

You can export a selected system certificate or a certificate and its associated private key. If you export a certificate and its private key for backup purposes, you can reimport them later if needed.

**Before you begin**
To perform the following task, you must be a Super Admin or System Admin.

---

**Step 1** Choose Administration > System > Certificates > System Certificates.

**Step 2** Check the checkbox next to the certificate that you want to export and then click **Export**.

**Step 3** Choose whether to export only the certificate, or the certificate and its associated private key.

**Tip** We do not recommend exporting the private key associated with a certificate because its value may be exposed. If you must export a private key (for example, when you export a wild card system certificate to be imported in to the other nodes for inter-node communication), specify an encryption password for the private key. You will need to specify this password while importing this certificate in to another Cisco ISE node to decrypt the private key.

**Step 4** Enter the password if you have chosen to export the private key. The password should be at least 8 characters long.

**Step 5** Click **Export** to save the certificate to the file system that is running your client browser.

If you export only the certificate, the certificate is stored in the privacy-enhanced mail format. If you export both the certificate and private key, the certificate is exported as a .zip file that contains the certificate in the privacy-enhanced mail format and the encrypted private key file.

---

**Trusted Certificates Store**

The Trusted Certificates Store contains X.509 certificates that are used for trust and for Simple Certificate Enrollment Protocol (SCEP).

The certificates in the Trusted Certificate Store are managed on the PAN, and are replicated to every node in the Cisco ISE deployment. Cisco ISE supports wildcard certificates.

Cisco ISE uses the trusted certificates for the following purposes:

- To verify client certificates used for authentication by endpoints, and by Cisco ISE administrators accessing ISE-PICThe Admin Portal using certificate-based administrator authentication.
To enable secure communication between Cisco ISE nodes in a deployment. The Trusted Certificates Store must contain the chain of CA certificates needed to establish trust with the system certificate on each node in a deployment.

- If a self-signed certificate is used for the system certificate, the self-signed certificate from each node must be placed in the Trusted Certificates Store of the PAN.
- If a CA-signed certificate is used for the system certificate, the CA root certificate, as well as any intermediate certificates in the trust chain, must be placed in the Trusted Certificates Store of the PAN.

To enable secure LDAP authentication, a certificate from the Certificate Store must be selected when defining an LDAP identity source that will be accessed over SSL.

To distribute to personal devices preparing to register in the network using the personal devices portals. Cisco ISE implements the SCEP on Policy Service Nodes (PSN) to support personal device registration. A registering device uses the SCEP protocol to request a client certificate from a PSN. The PSN contains a registration authority (RA) that acts as an intermediary; it receives and validates the request from the registering device, and then forwards the request to an external CA or the internal Cisco ISE CA, which issues the client certificate. The CA sends the certificate back to the RA, which returns it to the device.

Each SCEP CA used by Cisco ISE is defined by a SCEP RA Profile. When a SCEP RA Profile is created, two certificates are automatically added to the Trusted Certificates Store:

- A CA certificate (a self-signed certificate)
- An RA certificate (a Certificate Request Agent certificate), which is signed by the CA.

The SCEP protocol requires that these two certificates be provided by the RA to a registering device. By placing these two certificates in the Trusted Certificates Store, they are replicated to all PSN nodes for use by the RA on those nodes.

Note

If you remove the SCEP RA profile, which issues certificates signed by the CA that signs the certificates used in System Certificate for EAP Authentication, the trusted certificates used for EAP authentication will be removed from the Trusted Certificate store and EAP authentications will fail.

Note

- X.509 certificates imported to Cisco ISE must be in Privacy-Enhanced Mail (PEM) or Distinguished Encoding Rule (DER) format. Files containing a certificate chain, that is, a system certificate along with the sequence of trust certificates that sign it, can be imported, subject to certain restrictions.
- When assigning public wildcard certificates to the guest portal and importing sub-CA with root-CA certificates, the certificate chain is not sent until the ISE services are restarted.

ISE Community Resource

Install a Third-Party CA Certificate in ISE 2.0
Certificates in Trusted Certificates Store

The Trusted Certificate Store is prepopulated with trusted certificates: Manufacturing certificate, Root certificate, and other trusted certificates. The Root certificate (Cisco Root CA) signs the Manufacturing (Cisco CA Manufacturing) certificate. These certificates are disabled by default. If you have Cisco IP phones as endpoints in your deployment, you should enable these two certificates so the Cisco-signed client certificates for the phones can be authenticated.

Trusted Certificate Naming Constraint

A trusted certificate in CTL may contain a name constraint extension. This extension defines a namespace for values of all subject name and subject alternative name fields of subsequent certificates in a certificate chain. Cisco ISE does not check constraints specified in a root certificate.

The following name constraints are supported:

- Directory name
  The Directory name constraint should be a prefix of the directory name in subject/SAN. For example,
  - Correct subject prefix:
    CA certificate name constraint: Permitted: O=Cisco
    Client certificate subject: O=Cisco,CN=Salomon
  - Incorrect subject prefix:
    CA certificate name constraint: Permitted: O=Cisco
    Client certificate subject: CN=Salomon,O=Cisco

- DNS

- E-mail

- URI (The URI constraint must start with a URI prefix such as http://, https://, ftp://, or ldap://).

The following name constraints are not supported:

- IP address

- Othername

When a trusted certificate contains a constraint that is not supported and certificate that is being verified does not contain the appropriate field, it is rejected because Cisco ISE cannot verify unsupported constraints.

The following is an example of the name constraints definition within the trusted certificate:

```
X509v3 Name Constraints: critical
  Permitted:
    othername:<unsupported>
    email: abcde.at
    email: abcde.be
    email: abcde.bg
    email: abcde.by
    DNS:.dir
  DirName: DC = dir, DC = emea
  DirName: C = AT, ST = EMEA, L = AT, O = ABCDE Group, OU = Domestic
  DirName: C = BG, ST = EMEA, L = BG, O = ABCDE Group, OU = Domestic
```
An acceptable client certificate subject that matches the above definition is as follows:

Subject: DC=dir, DC=emea, OU=+DE, OU=OU-Administration, OU=Users, OU=X1, CN=cwinwell

**View Trusted Store Certificates**

The Trusted Certificates page lists all the trusted certificates that have been added to Cisco ISE. To view the trusted certificates, you must be a Super Admin or System Admin.

To view all the certificates, choose Choose Administration > System > Certificates > Trusted Certificates. The Trusted Certificates page appears, listing all the trusted certificates.

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

**Change the Status of a Certificate in Trusted Certificates Store**

The status of a certificate must be enabled so that Cisco ISE can use the certificate for establishing trust. When a certificate is imported into the Trusted Certificates Store, it is automatically enabled.

**Step 1**
Choose Administration > System > Certificates > Trusted Certificates.

**Step 2**
Check the checkbox next to the certificate you want to enable or disable, and click Edit.

**Step 3**
Change the status.

**Step 4**
Click Save.

**Add a Certificate to Trusted Certificates Store**

The Certificate Store page allows you to add CA certificates to Cisco ISE.

**Before you begin**

- To perform the following task, you must be a Super Admin or System Admin.

- Ensure that the certificate store certificate resides on the file system of the computer where your browser is running. The certificate must be in PEM or DER format.

- If you plan to use the certificate for Admin or EAP authentication, ensure that the basic constraints are defined in the certificate and the CA flag is set to true.

**Step 1**
Choose Administration > System > Certificates > Trusted Certificates.
Step 2 Click **Import**.

Step 3 Configure the field values as necessary.

If you plan to use any sub-CA certificate in the certificate chain for EAP authentication, ensure that you check the **Trust for client authentication** and **Syslog** checkbox while importing all the certificates in the certificate chain up until the Root CA.

When you change the authentication type from password-based authentication to certificate-based authentication, Cisco ISE restarts the application server on each node in your deployment, starting with the application server on the PAN and followed, one-by-one, by each additional node.

---

### Edit a Trusted Certificate

After you add a certificate to the Trusted Certificates Store, you can further edit it by using the edit settings.

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

---

### Step 1

Choose **Administration > System > Certificates > Trusted Certificates**.

### Step 2

Check the check box next to the certificate that you want to edit, and click **Edit**.

### Step 3

Modify the editable fields as required.

### Step 4

Click **Save** to save the changes you have made to the certificate store.

---

### Delete Trusted Certificates

You can delete trusted certificates that you no longer need. However, ensure that you do not delete the ISE Internal CA (Certificate Authority) certificates. The ISE Internal CA certificates can be deleted only when you replace the ISE Root Certificate Chain for the entire deployment.

---

### Step 1

Choose **Administration > System > Certificates > Trusted Certificates**.

### Step 2

Check the check boxes next to the certificates that you want to delete, and click **Delete**.

A warning message appears. If you have chosen to delete the ISE Internal CA certificates, click:

- **Delete**—To delete the ISE internal CA certificates. All endpoint certificates signed by the ISE Internal CA become invalid and the endpoints cannot get on to the network. To allow the endpoints on the network again, import the same ISE Internal CA Certificates into the Trusted Certificates store.
- **Delete & Revoke**—Deletes and revokes the ISE internal CA certificates. All endpoint certificates signed by the ISE Internal CA become invalid and the endpoints cannot get on to the network. This operation cannot be undone. You must replace the ISE Root Certificate Chain for the entire deployment.

### Step 3

Click **Yes** to delete the certificate.
Export a Certificate from the Trusted Certificates Store

Before you begin
To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose Administration > System > Certificates > Trusted Certificates.
Step 2 Check the check box next to the certificate that you want to export, and click Export. You can export only one certificate at a time.
Step 3 Save the privacy-enhanced mail file to the file system that is running your client browser.

Import the Root Certificates to the Trusted Certificate Store

While importing the root CA and intermediate CA certificates, you can specify the service(s) for which the Trusted CA certificates are to be used.

Before you begin
You must have the root certificate and other intermediate certificates from the Certificate Authority that signed your CSRs and returned the digitally signed CA certificates.

Step 1 Choose Administration > System > Certificates > Trusted Certificates.
Step 2 Click Import.
Step 3 Click Browse to select the root CA certificate.
Step 4 Enter a Friendly Name.
   If you do not enter a Friendly Name, Cisco ISE autopopulates this field with a Friendly Name of the format common-name#issuer#nnnnn, where nnnnn is a unique number. You can edit the certificate again to change the Friendly Name.
Step 5 Choose the root certificate returned by your CA.
Step 6 Check the check boxes next to the services for which you want to use this trusted certificate for.
Step 7 Enter a description.
Step 8 Click Submit.

What to do next
Import the intermediate CA certificates in to the Trusted Certificates store (if applicable).

Certificate Chain Import

You can import multiple certificates from a single file that contains a certificate chain received from a Certificate store. All certificates in the file must be in Privacy-Enhanced Mail (PEM) format, and the certificates must be arranged in the following order:
   • The last certificate in the file must be the client or server certificate being issued by the CA.
• All preceding certificates must be the root CA certificate plus any intermediate CA certificates in the signing chain for the issued certificate.

Importing a certificate chain is a two-step process:

1. Import the certificate chain file into the Trusted Certificate Store in the Admin portal. This operation imports all certificates from the file except the last one into the Trusted Certificates Store.
2. Import the certificate chain file using the Bind a CA-Signed Certificate operation. This operation imports the last certificate from the file as a local certificate.

Certificate Signing Requests

For a certificate authority (CA) to issue a signed certificate, you must create a certificate signing request (CSR) and submit it to the CA.

The list of Certificate Signing Requests (CSRs) that you have created is available in the Certificate Signing Requests page. To obtain signatures from a Certificate Authority (CA), you must export the CSRs and then send the certificates to the CA. The CA signs and returns your certificates.

You can manage the certificates centrally from the Admin portal. You can create CSRs for all nodes in the deployment and export them. Then you should submit the CSRs to a CA, obtain the CA-signed certificates from the CA, import the root and intermediary CA certificates returned by the CA in to the Trusted Certificates Store, and bind the CA-signed certificates to the CSRs.

Create a Certificate Signing Request and Submit the CSR to a Certificate Authority

You can generate a certificate signing request (CSR) to obtain a CA-signed certificate for the nodes in your deployment. You can generate the CSR for select nodes in the deployment or for all the nodes in your deployment.

Step 1 Choose Administration > System > Certificates > Certificate Signing Requests
Step 2 Enter the values for generating a CSR. See Certificate-Signing Request Settings, on page 926 for information on each of the fields.
Step 3 Click Generate to generate the CSR.
The CSR is generated.
Step 4 Click Export to open the CSR in a Notepad.
Step 5 Copy all the text from “-----BEGIN CERTIFICATE REQUEST-----” through “-----END CERTIFICATE REQUEST-----.”
Step 6 Paste the contents of the CSR in to the certificate request of a chosen CA.
Step 7 Download the signed certificate.

Some CAs might email the signed certificate to you. The signed certificate is in the form of a zip file that contains the newly issued certificate and the public signing certificates of the CA that you must add to the Cisco ISE trusted certificates store. The digitally-signed CA certificate, root CA certificate, and other intermediate CA certificate (if applicable) are downloaded to the local system running your client browser.
Bind the CA-Signed Certificate to the CSR

After you have the digitally signed certificate returned by the CA, you must bind it to the certificate signing request (CSR). You can perform the bind operation for all the nodes in your deployment from the Admin portal.

Before you begin

- You must have the digitally signed certificate, and the relevant root intermediate CA certificates returned by the CA.
- Import the relevant root and intermediate CA certificates in to the Trusted Certificates Store (Administration > System > Certificates > Trusted Certificates).

Step 1 Choose Administration > System > Certificates > Certificate Signing Requests

Check the check box next to the node for which you are binding the CSR with the CA-signed certificate.

Step 2 Click Bind.

Step 3 Click Browse to choose the CA-signed certificate.

Step 4 Specify a Friendly Name for the certificate.

Step 5 Check the Validate Certificate Extensions check box if you want Cisco ISE to validate certificate extensions.

If you enable the Validate Certificate Extensions option, and the certificate that you are importing contains a basic constraints extension with the CA flag set to true, ensure that the key usage extension is present, and that the keyEncipherment bit or the keyAgreement bit, or both, are also set.

Note ISE requires EAP-TLS client certificates to have digital signature key usage extension.

Step 6 Check the service for which this certificate will be used in the Usage area.

This information is autopopulated, if you have enabled the Usage option while generating the CSR. If you do not want to specify the usage at the time of binding the certificate, uncheck the Usage option. You can edit the certificate later and specify the usage.

Step 7 Click Submit to bind the CA-signed certificate.

If you have chosen to use this certificate for Cisco ISE internode communication, the application server on the Cisco ISE node is restarted.

Repeat this process to bind the CSR with the CA-signed certificate on the other nodes.

What to do next

Import the Root Certificates to the Trusted Certificate Store, on page 155

Export a Certificate Signing Request

You can use this page to export certificate signing requests.
Before you begin

To perform the following task, you must be a Super Admin or System Admin.

---

**Step 1**  Choose Administration > System > Certificates > Certificate Signing Requests

**Step 2**  Check the check box next to the certificates that you want to export, and click Export.

**Step 3**  Click OK to save the file to the file system that is running the client browser.

---

**Install Trusted Certificates for Cisco ISE Inter-node Communication**

When you set up the deployment, before you register a secondary node, you must populate the PAN’s Certificate Trust List (CTL) with appropriate CA certificates that are used to validate the Admin certificate of the secondary node. The procedure to populate the CTL of the PAN is different for different scenarios:

- If the secondary node is using a CA-signed certificate to communicate with the Admin portal, you must import the CA-signed certificate of the secondary node, the relevant intermediate certificates (if any), and the root CA certificate (of the CA that signed the secondary node’s certificate) in to the CTL of the PAN.

- If the secondary node is using a self-signed certificate to communicate with the Admin portal, you can import the self-signed certificate of the secondary node in to the CTL of the PAN.

---

**Note**

- If you change the Admin certificate on a registered secondary node, you must obtain appropriate CA certificates that can be used to validate the secondary node’s Admin certificate and import it in to the CTL of the PAN.

- If you use self-signed certificates to secure communication between a client and PSN in a deployment, when BYOD users move from one location to another, EAP-TLS user authentication fails. For such authentication requests that have to be serviced between a few PSNs, you must secure communication between the client and PSN with an externally-signed CA certificate or use wildcard certificates signed by an external CA.

---

Ensure that the certificate issued by the external CA has basic constraints defined and the CA flag set to true. To install CA-signed certificates for inter-node communication:

---

**Step 1**  Create a Certificate Signing Request and Submit the CSR to a Certificate Authority, on page 156

**Step 2**  Import the Root Certificates to the Trusted Certificate Store, on page 155

**Step 3**  Bind the CA-Signed Certificate to the CSR, on page 157

---
Set Up Certificates for Portal Use

With multiple Policy Service nodes (PSNs) in a deployment that can service a web portal request, Cisco ISE needs a unique identifier to identify the certificate that has to be used for portal communication. When you add or import certificates that are designated for portal use, you must define a certificate group tag and associate it with the corresponding certificate on each node in your deployment. You must associate this certificate group tag to the corresponding end-user portals (guest, sponsor, and personal devices portals). This certificate group tag is the unique identifier that helps Cisco ISE identify the certificate that has to be used when communicating with each of these portals. You can designate one certificate from each node for each of the portals.

![Note]
Cisco ISE presents the Portal certificate on TCP port 8443 (or the port that you have configured for portal use).

---

**Step 1**
Create a Certificate Signing Request and Submit the CSR to a Certificate Authority, on page 156.

You must choose a Certificate Group Tag that you have already defined or create a new one for the portal. For example, mydevicesportal.

**Step 2**
Import the Root Certificates to the Trusted Certificate Store, on page 155.

**Step 3**
Bind the CA-Signed Certificate to the CSR, on page 157.

---

Reassign Default Portal Certificate Group Tag to CA-Signed Certificate

By default, all Cisco ISE portals use the self-signed certificate. If you want to use a CA-signed certificate for portals, you can assign the default portal certificate group tag to a CA-signed certificate. You can use an existing CA-signed certificate or generate a CSR and obtain a new CA-signed certificate for portal use. You can reassign any portal group tag from one certificate to another.

![Note]
When you edit an existing certificate, if the portal tag (guest) that is associated with the certificate is already in use by any of the portals, then you cannot reassign the default portal certificate group tag or any other portal group tag to this certificate. The system displays the list of portals that use the "guest" portal tag.

The following procedure describes how to reassign the default portal certificate group tag to a CA-signed certificate.

---

**Step 1**
Choose Administration > System > Certificates > System Certificates.

Hover the mouse over the i icon next to the Default Portal Certificate Group tag to view the list of portals that use this tag. You can also view the ISE nodes in the deployment that have portal certificates which are assigned this tag.

**Step 2**
Check the check box next to the CA-signed certificate that you want to use for portals, and click Edit.

Be sure to choose a CA-signed certificate that is not in use by any of the portals.
Step 3  Under the Usage area, check the Portal check box and choose the Default Portal Certificate Group Tag.

Step 4  Click Save.

A warning message appears.

Step 5  Click Yes to reassign the default portal certificate group tag to the CA-signed certificate.

### Associate the Portal Certificate Tag Before You Register a Node

If you use the "Default Portal Certificate Group" tag for all the portals in your deployment, before you register a new ISE node, ensure that you import the relevant CA-signed certificate, choose "Portal" as a service, and associate the "Default Portal Certificate Group" tag with this certificate.

When you add a new node to a deployment, the default self-signed certificate is associated with the "Default Portal Certificate Group" tag and the portals are configured to use this tag.

After you register a new node, you cannot change the Certificate Group tag association. Therefore, before you register the node to the deployment, you must do the following:

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a self-signed certificate, choose &quot;Portal&quot; as a service, and assign a different certificate group tag (for example, tempportaltag).</td>
</tr>
<tr>
<td>2</td>
<td>Change the portal configuration to use the newly created certificate group tag (tempportaltag).</td>
</tr>
<tr>
<td>3</td>
<td>Edit the default self-signed certificate and remove the Portal role.</td>
</tr>
<tr>
<td>4</td>
<td>This option removes the Default Portal Certificate Group tag association with the default self-signed certificate.</td>
</tr>
</tbody>
</table>

### Do one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Generate a CSR | When you generate the CSR:  
  1. Choose "Portal" as a service for which you will use this certificate and associate the "Default Portal Certificate Group" tag.  
  2. Send the CSR to a CA and obtain the signed certificate.  
  3. Import the root and any other intermediate certificates of the CA that signed your certificate into the Trusted Certificates store.  
  4. Bind the CA-signed certificate with the CSR. |

| Import the private key and the CA-signed certificate | When you import the CA-signed certificate:  
  1. Choose "Portal" as a service for which you will use this certificate and associate the "Default Portal Certificate Group" tag.  
  2. Import the root and any other intermediate certificates of the CA that signed your certificate into the Trusted Certificates store. |

| Edit an existing CA-signed certificate. | When you edit the existing CA-signed certificate:  
  Choose "Portal" as a service for which you will use this certificate and associate the "Default Portal Certificate Group" tag. |
**Step 5** Register the ISE node to the deployment.
The portal configuration in the deployment is configured to the "Default Portal Certificate Group" tag and the portals are configured to use the CA-signed certificate associated with the "Default Portal Certificate Group" tag on the new node.

---

**User and Endpoint Certificate Renewal**

By default, Cisco ISE rejects a request that comes from a device whose certificate has expired. However, you can change this default behavior and configure ISE to process such requests and prompt the user to renew the certificate.

If you choose to allow the user to renew the certificate, Cisco recommends that you configure an authorization policy rule which checks if the certificate has been renewed before processing the request any further. Processing a request from a device whose certificate has expired may pose a potential security threat. Hence, you must configure appropriate authorization profiles and rules to ensure that your organization’s security is not compromised.

Some devices allow you to renew the certificates before and after their expiry. But on Windows devices, you can renew the certificates only before it expires. Apple iOS, Mac OSX, and Android devices allow you to renew the certificates before or after their expiry.

**Dictionary Attributes Used in Policy Conditions for Certificate Renewal**

Cisco ISE certificate dictionary contains the following attributes that are used in policy conditions to allow a user to renew the certificate:

- **Days to Expiry**: This attribute provides the number of days for which the certificate is valid. You can use this attribute to create a condition that can be used in authorization policy. This attribute can take a value from 0 to 15. A value of 0 indicates that the certificate has already expired. A value of 1 indicates that the certificate has less than 1 day before it expires.

- **Is Expired**: This Boolean attribute indicates whether a certificate has expired or not. If you want to allow certificate renewal only when the certificate is near expiry and not after it has expired, use this attribute in authorization policy condition.

**Authorization Policy Condition for Certificate Renewal**

You can use the CertRenewalRequired simple condition (available by default) in authorization policy to ensure that a certificate (expired or about to expire) is renewed before Cisco ISE processes the request further.

**CWA Redirect to Renew Certificates**

If a user certificate is revoked before its expiry, Cisco ISE checks the CRL published by the CA and rejects the authentication request. In case, if a revoked certificate has expired, the CA may not publish this certificate in its CRL. In this scenario, it is possible for Cisco ISE to renew a certificate that has been revoked. To avoid this, before you renew a certificate, ensure that the request gets redirected to Central Web Authentication (CWA) for a full authentication. You must create an authorization profile to redirect the user for CWA.

**Configure Cisco ISE to Allow Users to Renew Certificates**

You must complete the tasks listed in this procedure to configure Cisco ISE to allow users to renew certificates.
Before you begin
Configure a limited access ACL on the WLC to redirect a CWA request.

Step 1 Update the Allowed Protocol Configuration, on page 162
Step 2 Create an Authorization Policy Profile for CWA Redirection, on page 162
Step 3 Create an Authorization Policy Rule to Renew Certificates, on page 163
Step 4 Enable BYOD Settings in the Guest Portal, on page 163

Update the Allowed Protocol Configuration

Step 1 Choose Policy > Policy Elements > Results > Authentication > Allowed Protocols > Default Network Access.
Step 2 Check the Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy check box under the EAP-TLS protocol and EAP-TLS inner methods for PEAP and EAP-FAST protocols.
Requests that use the EAP-TLS protocol will go through the NSP flow.
For PEAP and EAP-FAST protocols, you must manually configure Cisco AnyConnect for Cisco ISE to process the request.
Step 3 Click Submit.

What to do next
Create an Authorization Policy Profile for CWA Redirection, on page 162

Create an Authorization Policy Profile for CWA Redirection

Before you begin
Ensure that you have configured a limited access ACL on the WLC.

Step 1 Choose Policy > Policy Elements > Results > Authorization > Authorization Profiles.
Step 2 Click Add.
Step 3 Enter a name for the authorization profile. For example, CertRenewal_CWA.
Step 4 Check the Web Redirection (CWA, DRW, MDM, NSP, CPP) check box in the Common Tasks area.
Step 5 Choose Centralized Web Auth from the drop-down list and the limited access ACL.
Step 6 Check the Display Certificates Renewal Message check box.
The URL-redirect attribute value changes and includes the number of days for which the certificate is valid.
Step 7 Click Submit.
If you have configured the following Device Registration WebAuth (DRW) policies for wireless devices in Cisco ISE 1.2:

- DRW-Redirect policy with Condition = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) and Profile = Wireless-drw-redirect
- DRW-Allow policy with Condition = (Wireless_MAB AND Network Access:UseCase EQUALS HostLookup) and Profile = Wireless-Permit

After upgrading to ISE 1.3 or above version, you must update the DRW-Allow policy condition as follows:

- Condition = (Wireless_MAB AND Network Access:UseCase EQUALSGuest Flow) and Profile = Wireless-Permit

**What to do next**

Create an Authorization Policy Rule to Renew Certificates, on page 163

### Create an Authorization Policy Rule to Renew Certificates

**Before you begin**

Ensure that you have created an authorization profile for central web authentication redirection.

Enable Policy Sets on Administration > System > Settings > Policy Settings.

**Step 1** Choose Work Centers > Device Administration > Policy Sets.

**Step 2** Click Create Above.

**Step 3** Enter a name for the new rule.

**Step 4** Choose the following simple condition and result:

If CertRenewalRequired EQUALS True, then choose the authorization profile that you created earlier (CertRenewal_CWA) for the permission.

**Step 5** Click Save.

**What to do next**

When you access the corporate network with a device whose certificate has expired, click Renew to reconfigure your device.

### Enable BYOD Settings in the Guest Portal

For a user to be able to renew a personal device certificate, you must enable the BYOD settings in the chosen guest portal.

**Step 1** Choose Work Centers > Guest Access > Portals & Components > Guest Portals.
a) Select the chosen CWA portal and click **Edit**.

**Step 2** From BYOD Settings, check the **Allow employees to use personal devices on the network** check box.

**Step 3** Click **Save**.

---

**Certificate Renewal Fails for Apple iOS Devices**

When you use ISE to renew the endpoint certificates on Apple iOS devices, you might see a “Profiled Failed to Install” error message. This error message appears if the expiring or expired network profiles were signed by a different Admin HTTPS certificate than the one that is used in processing the renewal, either on the same Policy Service Node (PSN) or on another PSN.

As a workaround, use a multi-domain SSL certificate, which is commonly referred to as Unified Communications Certificate (UCC), or a wildcard certificate for Admin HTTPS on all PSNs in the deployment.

---

**Cisco ISE CA Service**

Certificates can be self-signed or digitally signed by an external Certificate Authority (CA). The Cisco ISE Internal Certificate Authority (ISE CA) issues and manages digital certificates for endpoints from a centralized console to allow employees to use their personal devices on the company's network. A CA-signed digital certificate is considered industry standard and more secure. The Primary PAN is the Root CA. The Policy Service Nodes (PSNs) are subordinate CAs to the Primary PAN (SCEP RA). The ISE CA offers the following functionalities:

- **Certificate Issuance**: Validates and signs Certificate Signing Requests (CSRs) for endpoints that connect to your network.
- **Key Management**: Generates and securely stores keys and certificates on both PAN and PSN nodes.
- **Certificate Storage**: Stores certificates issued to users and devices.
- **Online Certificate Status Protocol (OCSP) Support**: Provides an OCSP responder to check for the validity of certificates.

---

**ISE CA Certificates Provisioned on Administration and Policy Service Nodes**

After installation, a Cisco ISE node is provisioned with a Root CA certificate, and a Node CA certificate to manage certificates for endpoints.
When you set up a deployment, the node that you designate as the Primary Administration Node (PAN) becomes the Root CA. The PAN has a Root CA certificate and a Node CA certificate that is signed by the Root CA.

When you register a Secondary Administration Node to the PAN, a Node CA certificate is generated and is signed by the Root CA on the Primary Administration Node.

Any Policy Service Node (PSN) that you register with the PAN is provisioned an Endpoint CA and an OCSP certificate signed by the Node CA of the PAN. The Policy Service Nodes (PSNs) are subordinate CAs to the PAN. When you use the ISE CA, the Endpoint CA on the PSN issues the certificates to the endpoints that access your network.
ISE CA Chain Regeneration

When you regenerate the Cisco ISE CA chain, all the certificates including the Root CA, Node CA, and Endpoint CA certificates are regenerated. You must regenerate the ISE CA chain when you change the domain name or hostname of your PAN or PSN. When you upgrade from earlier releases to Release 2.0 or later, we recommend that you regenerate the ISE CA chain to move from the two root hierarchy to a single root hierarchy.

Elliptical Curve Cryptography Certificates Support

Cisco ISE CA service supports certificates based on Elliptical Curve Cryptography (ECC) algorithms. ECC offers increased security and better performance than other cryptographic algorithms while providing the same level of security as other systems with a much smaller key size.

The key size needed for encryption and digital signatures is far less than other systems. The following table shows the key sizes of ECC and RSA to provide comparable security strengths.

<table>
<thead>
<tr>
<th>ECC Key Size (in bits)</th>
<th>RSA Key Size (in bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>160</td>
<td>1024</td>
</tr>
<tr>
<td>224</td>
<td>2048</td>
</tr>
<tr>
<td>256</td>
<td>3072</td>
</tr>
<tr>
<td>384</td>
<td>7680</td>
</tr>
<tr>
<td>521</td>
<td>15360</td>
</tr>
</tbody>
</table>

Given the smaller key size, this system requires less time for encryption and hence offers better performance.

Cisco ISE supports the following ECC curve types. The higher the curve type or key size, the greater is the security.

- P-192
- P-256
- P-384
- P-521

Cisco ISE CA service supports ECC certificates for devices connecting through the BYOD flow. You can also generate ECC certificates from the Certificate Provisioning Portal.
The following table lists the operating systems and versions that support ECC along with the curve types that are supported. If your devices are not running a supported operating system or on a supported version, you can use RSA-based certificates instead.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Supported Versions</th>
<th>Supported Curve Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>8 and later</td>
<td>P-256, P-384, and P-521</td>
</tr>
<tr>
<td>Android</td>
<td>4.4 and later</td>
<td>All curve types (except Android 6.0, which does not support the P-192 curve type).</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td></td>
<td>Android 6.0 requires May 2016 patch to support ECC certificates.</td>
</tr>
</tbody>
</table>

Windows 7 and Apple iOS do not natively support ECC for EAP-TLS authentication. This release of Cisco ISE does not support the use of ECC certificates on MAC OS X devices.

If the BYOD flow with Enrollment over Secure Transport (EST) protocol is not working properly, check the following:

- Certificate Services Endpoint Sub CA certificate chain is complete. To check whether the certificate chain is complete:
  1. Choose Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates.
  2. Check the check box next to the certificate that you want to check and click View.

- Ensure that the CA and EST services are up and running. If the services are not enabled, go to Administration > System > Certificates > Certificate Authority > Internal CA Settings to enable the CA service.

- If you have upgraded to Cisco ISE 2.1 from an ISE version prior to 2.0, replace the ISE Root CA certificate chain after the upgrade. To do this:
  2. Click Generate Certificate Signing Requests (CSR).
  3. Choose ISE Root CA from the Certificate(s) will be used for drop-down list.
  4. Click Replace ISE Root CA Certificate Chain.

This release of Cisco ISE does not support EST clients to authenticate directly against the EST Server residing within Cisco ISE.

During the on-boarding on an Android or a Windows endpoint, an EST flow is triggered internally within ISE if the request is for an ECC-based certificate.
Cisco ISE Certificate Authority Certificates

The Certificate Authority (CA) Certificates page lists all the certificates related to the internal Cisco ISE CA. In previous releases, these CA certificates were present in the Trusted Certificates store and are now moved to the CA Certificates page. These certificates are listed node wise in this page. You can expand a node to view all the ISE CA certificates of that particular node. The Primary and Secondary Administration nodes have the root CA, node CA, subordinate CA, and OCSP responder certificates. The other nodes in the deployment have the endpoint subordinate CA and OCSP certificates.

When you enable the Cisco ISE CA service, these certificates are generated and installed on all the nodes automatically. Also, when you replace the entire ISE Root CA Chain, these certificates are regenerated and installed on all the nodes automatically. There is no manual intervention required.

The Cisco ISE CA certificates follow the following naming convention: Certificate Services <Endpoint Sub CA/Node CA/Root CA/OCSP Responder> <node_hostname>#certificate_number.

From the CA Certificates page, you can edit, import, export, delete, and view the Cisco ISE CA certificates.

Edit a Cisco ISE CA Certificate

After you add a certificate to the Cisco ISE CA Certificates Store, you can further edit it by using the edit settings.

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

---

**Step 1**  
Choose Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates.

**Step 2**  
Check the check box next to the certificate that you want to edit, and click Edit.

**Step 3**  
Modify the editable fields as required. See Edit Certificate Settings, on page 934 for a description of the fields.

**Step 4**  
Click Save to save the changes you have made to the certificate store.

---

Export a Cisco ISE CA Certificate

To export the Cisco ISE root CA and node CA certificates:

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

---

**Step 1**  
Choose Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates.

**Step 2**  
Check the check box next to the certificate that you want to export, and click Export. You can export only one certificate at a time.

**Step 3**  
Save the privacy-enhanced mail file to the file system that is running your client browser.
Import a Cisco ISE CA Certificate

If an endpoint tries to authenticate to your network using a certificate issued by Cisco ISE CA from another deployment, you must import the Cisco ISE root CA, node CA, and endpoint sub CA certificates from that deployment into the Cisco ISE Trusted Certificates store.

Before you begin

• To perform the following task, you must be a Super Admin or System Admin.

• Export the ISE root CA, node CA, and endpoint sub CA certificates from the deployment where the endpoint certificate is signed and store it on the file system of the computer where your browser is running.

Step 1
Log in to the Admin Portal of the deployment where the endpoint is getting authenticated.

Step 2
Choose Administration > System > Certificates > Trusted Certificates.

Step 3
Click Import.

Step 4
Configure the field values as necessary. See Trusted Certificate Import Settings, on page 936 for more information.

If client certificate-based authentication is enabled, then Cisco ISE will restart the application server on each node in your deployment, starting with the application server on the PAN and followed, one-by-one, by each additional node.

Certificate Templates

Certificate templates contain properties that are common to all certificates issued by the Certificate Authority (CA) based on that template. The certificate template defines the Subject, Subject Alternative Name (SAN), key type, key size, SCEP RA profile that must be used, validity period of the certificate, and the extended key usage (EKU) that specifies whether the certificate has to be used for client or server authentication or both. The internal Cisco ISE CA (ISE CA) uses a certificate template to issue certificates based on that template.

Cisco ISE comes with the following default certificate templates for the ISE CA. You can create additional certificate templates, if needed. The default certificate templates are:

• CA_SERVICE_Certificate_Template—For other network services that use Cisco ISE as the Certificate Authority. For example, use this certificate template while configuring ISE to issue certificates for ASA VPN users. You can modify only the validity period in this certificate template.

• EAP_Authentication_Certificate_Template—For EAP authentication.

• pxGrid_Certificate_Template—For the pxGrid controller while generating the certificate from the Certificate Provisioning Portal.

Certificate Template Name Extension

The Cisco ISE Internal CA includes an extension to represent the certificate template that was used to create the endpoint certificate. All endpoint certificates issued by the internal CA contain a certificate template name extension. This extension represents the certificate template that was used to create that endpoint certificate. The extension ID is 1.3.6.1.4.1.9.21.2.5. You can use the CERTIFICATE: Template Name attribute in authorization policy conditions and assign appropriate access privileges based on the results of the evaluation.
Use Certificate Template Name in Authorization Policy Conditions

You can use the certificate template name extension in authorization policy rules.

---

**Step 1** Choose *Policy > Policy Sets*, and expand the Default policy set to view the authorization policy rules.

**Step 2** Add a new rule or edit an existing rule. This example describes editing the Compliant_Device_Access rule:

a) Edit the Compliant_Device_Access rule.
b) Choose *Add Attribute/Value*.
c) From Dictionaries, choose the *CERTIFICATE: Template Name* attribute and *Equals* operator.
d) Enter the value of the certificate template name. For example, EAP_Authentication_Certificate_Template.

**Step 3** Click *Save*.

---

Deploy Cisco ISE CA Certificates for pxGrid Controller

Cisco ISE CA provides a certificate template for the pxGrid controller to generate a certificate from the Certificate Provisioning Portal.

**Before you begin**

Generate a certificate signing request (CSR) for the pxGrid client and copy the contents of the CSR in to the clipboard.

---

**Step 1** Create a network access user account (Administration > Identity Management > Identities > Users > Add).

Make note of the user group to which the user is assigned.


a) Select the certificate provisioning portal and click *Edit*.
b) Click the *Portal Settings* drop-down list. From the Configure authorized groups Available list, select the user group to which the network access user belongs to and move it to Chosen list.
d) Save the portal settings.

**Step 3** Launch the Certificate Provisioning Portal. Click the Portal Test URL link.

a) Log in to the Certificate Provisioning Portal using the user account created in step 1.
b) Accept the AUP and click *Continue*.
c) From the *I want to* drop-down list, choose *Generate a single certificate (with certificate signing request)*.
d) In the Certificate Signing Request Details field, paste the contents of the CSR from the clipboard.
e) From the *Certificate Download Format* drop-down list, choose *PKCS8 format*.

**Note** If you choose the PKCS12 format, you must convert the single certificate file in to separate certificate and key files. The certificate and key files must be in binary DER encoded or PEM format before you can import them in to Cisco ISE.

f) From the *Choose Certificate Template* drop-down list, choose *pxGrid_Certificate_Template*.
g) Enter a certificate password.
h) Click Generate.
   The certificate is generated.

i) Export the certificate.
   The certificate along with the certificate chain is exported.

Step 4  Import the Cisco ISE CA chain into the Trusted Certificates store in the pxGrid client.

---

**Simple Certificate Enrollment Protocol Profiles**

To help enable certificate provisioning functions for the variety of mobile devices that users can register on the network, Cisco ISE enables you to configure one or more Simple Certificate Enrollment Protocol (SCEP) Certificate Authority (CA) profiles (called as Cisco ISE External CA Settings) to point Cisco ISE to multiple CA locations. The benefit of allowing for multiple profiles is to help ensure high availability and perform load balancing across the CA locations that you specify. If a request to a particular SCEP CA goes unanswered three consecutive times, Cisco ISE declares that particular server unavailable and automatically moves to the CA with the next lowest known load and response times, then it begins periodic polling until the server comes back online.


**Issued Certificates**

The Admin portal lists all the certificates issued by the internal ISE CA to endpoints (Administration > System > Certificates > Endpoint Certificates). The Issued Certificates page provides you an at-a-glance view of the certificate status. You can mouse over the Status column to find out the reason for revocation if a certificate has been revoked. You can mouse over the Certificate Template column to view additional details such as Key Type, Key Size or Curve Type, Subject, Subject Alternative Name (SAN), and Validity of the certificate. You can click on the endpoint certificate to view the certificate.

All certificates issued by the ISE CA (certificates automatically provisioned through the BYOD flow and certificates obtained from the Certificate Provisioning portal) are listed in the Endpoint Certificates page. You can manage these certificates from this page.

For example, if you want to view the certificates issued to user7, enter user7 in the text box that appears below the Friendly Name field. All the certificates issued by Cisco ISE to this user appear. Remove the search term from the text box to cancel the filter. You can also use the Advanced Filter option to view records based on various search criteria.

This Endpoint Certificates page also provides you the option to revoke an endpoint certificate, if necessary.

The Certificate Management Overview page displays the total number of endpoint certificates issued by each PSN node in your deployment. You can also view the total number of revoked certificates per node and the total number of certificates that have failed. You can filter the data on this page based on any of the attributes.

---

**Note**

pxGrid certificates are not listed in the Issued Certificates page.
Backup and Restore of Cisco ISE CA Certificates and Keys

You must back up the Cisco ISE CA certificates and keys securely to be able to restore them back on a Secondary Administration Node in case of a PAN failure and you want to promote the Secondary Administration Node to function as the root CA or intermediate CA of an external PKI. The Cisco ISE configuration backup does not include the CA certificates and keys. Instead, you should use the Command Line Interface (CLI) to export the CA certificates and keys to a repository and to import them. The `application configure ise` command now includes export and import options to backup and restore CA certificates and keys.

The following certificates from the Trusted Certificates Store are restored on the Secondary Administration Node:

- Cisco ISE Root CA certificate
- Cisco ISE Sub CA certificate
- Cisco ISE Endpoint RA certificate
- Cisco ISE OCSP Responder certificate

You must back up and restore Cisco ISE CA certificates and keys when you:

- Have a Secondary Administration Node in the deployment
- Replace the entire Cisco ISE CA root chain
- Configure Cisco ISE root CA to act as a subordinate CA of an external PKI
- Upgrade from Release 1.2 to a later release
- Restore data from a configuration backup. In this case, you must first regenerate the Cisco ISE CA root chain and then back up and restore the ISE CA certificates and keys.

Export Cisco ISE CA Certificates and Keys

You must export the CA certificates and keys from the PAN to import them on the Secondary Administration Node. This option enables the Secondary Administration Node to issue and manage certificates for endpoints when the PAN is down and you promote the Secondary Administration Node to be the PAN.

**Before you begin**

Ensure that you have created a repository to store the CA certificates and keys.

---

**Step 1**

Enter `application configure ise` command from the Cisco ISE CLI.

**Step 2**

Enter 7 to export the certificates and keys.

**Step 3**

Enter the repository name.

**Step 4**

Enter an encryption key.

A success message appears with the list of certificates that were exported, along with the subject, issuer, and serial number.

**Example:**

The following 4 CA key pairs were exported to repository 'sftp' at 'ise_ca_key_pairs_of_ise-vm1':

Subject:CN=Cisco ISE Self-Signed CA of ise-vm1
Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x621867df-568341cd-944cc77f-c9820765
Subject: CN=Cisco ISE Endpoint CA of ise-vm1
Issuer: CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#: 0x7027269d-d80a406d-831d5c26-f5e105fa

Subject: CN=Cisco ISE Endpoint RA of ise-vm1
Issuer: CN=Cisco ISE Endpoint CA of ise-vm1
Serial#: 0x1a65ec14-4f284da7-9532f0a0-8ae0e5c2

Subject: CN=Cisco ISE OCSP Responder Certificate of ise-vm1
Issuer: CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#: 0x6f6d4097-21f74c4d-8832ba95-4c320fb1

ISE CA keys export completed successfully

Import Cisco ISE CA Certificates and Keys

After you register the Secondary Administration Node, you must export the CA certificates and keys from the PAN and import them into the Secondary Administration Node.

Step 1 Enter **application configure ise** command from the Cisco ISE CLI.
Step 2 Enter 8 to import the CA certificates and keys.
Step 3 Enter the repository name.
Step 4 Enter the name of the file that you want to import.
Step 5 Enter the encryption key to decrypt the file.

A success message appears.

Example:

The following 4 CA key pairs were imported:
Subject: CN=Cisco ISE Self-Signed CA of ise-vm1
Issuer: CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#: 0x21ce1000-8008472c-a6bc4fd9-272c8da4

Subject: CN=Cisco ISE Endpoint CA of ise-vm1
Issuer: CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#: 0x05fa86d0-092542b4-8ff68ed4-f1964a56

Subject: CN=Cisco ISE Endpoint RA of ise-vm1
Issuer: CN=Cisco ISE Endpoint CA of ise-vm1
Serial#: 0x77932e02-e8c84b3d-b27e2f1c-e9f246ca

Subject: CN=Cisco ISE OCSP Responder Certificate of ise-vm1
Issuer: CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#: 0x5082017f-330e412f-8d83305d-e13fd2a5

Stopping ISE Certificate Authority Service...
Starting ISE Certificate Authority Service...
ISE CA keys import completed successfully
Generate Root CA and Subordinate CAs on the Primary PAN and PSN

When you set up the deployment, Cisco ISE generates a root CA on the Primary PAN and subordinate CA certificates on the Policy Service Nodes (PSNs) for the Cisco ISE CA service. However, when you change the domain name or the hostname of the Primary PAN or PSN, you must regenerate root CA on the Primary PAN and sub CAs on the PSNs respectively.

If you want to change the hostname on a PSN, instead of regenerating the root CA and subordinate CAs on the Primary PAN and PSNs respectively, you can deregister the PSN before changing the hostname, and register it back. A new subordinate certificate gets provisioned automatically on the PSN.

**Step 1**  
Administration > System > Certificates > Certificate Signing Requests

**Step 2**  
Click Generate Certificate Signing Requests (CSR).

**Step 3**  
Choose ISE Root CA from the Certificate(s) will be used for drop-down list.

**Step 4**  
Click Replace ISE Root CA Certificate chain.

The root CA and subordinate CA certificates get generated for all the nodes in your deployment.

**What to do next**

If you have a Secondary PAN in the deployment, obtain a backup of the Cisco ISE CA certificates and keys from the Primary PAN and restore it on the Secondary PAN. This ensures that the Secondary PAN can function as the root CA in case of a Primary PAN failure and you promote the Secondary PAN to be the Primary PAN.

Configure Cisco ISE Root CA as Subordinate CA of an External PKI

If you want the root CA on the Primary PAN to act as a subordinate CA of an external PKI, generate an ISE intermediate CA certificate signing request, send it to the external CA, obtain the root and CA-signed certificates, import the root CA certificate into the Trusted Certificates Store, and bind the CA-signed certificate to the CSR. In this case, the external CA is the root CA, the Primary PAN is a subordinate CA of the external CA, and the PSNs are subordinate CAs of the Primary PAN.

**Step 1**  
Choose Administration > System > Certificates > Certificate Signing Requests.

**Step 2**  
Click Generate Certificate Signing Requests (CSR).

**Step 3**  
Choose ISE Intermediate CA from the Certificate(s) will be used for drop-down list.

**Step 4**  
Click Generate.

**Step 5**  
Export the CSR, send it to the external CA, and obtain the CA-signed certificate.

**Step 6**  
Import the root CA certificate from the external CA in to the Trusted Certificates store.

**Step 7**  
Bind the CA-signed certificate with the CSR.

**What to do next**

If you have a Secondary PAN in the deployment, obtain a backup of the Cisco ISE CA certificates and keys from the Primary PAN and restore it on the Secondary PAN. This ensures that the Secondary PAN can function.
as subordinate CA of the external PKI in case of a Primary PAN failure and you promote the Secondary PAN
to be the Primary PAN.

**Configure Cisco ISE to Use Certificates for Authenticating Personal Devices**

You can configure Cisco ISE to issue and manage certificates for endpoints (personal devices) that connect
to your network. You can use the internal Cisco ISE Certificate Authority (CA) service to sign the certificate
signing request (CSR) from endpoints or forward the CSR to an external CA.

**Before you begin**

- Obtain a backup of the Cisco ISE CA certificates and keys from the Primary PAN and store them in a
  secure location for disaster recovery purposes.
- If you have a Secondary PAN in the deployment, back up the Cisco ISE CA certificates and keys from
  the Primary PAN and restore them on the Secondary PAN.

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Add Users to the Employee User Group, on page 175</td>
</tr>
<tr>
<td></td>
<td>You can add users to the internal identity store or to an external identity store such as Active Directory.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Create a Certificate Authentication Profile for TLS-Based Authentication, on page 176</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Create an Identity Source Sequence for TLS-Based Authentication, on page 176</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Creating a client provisioning policy.</td>
</tr>
<tr>
<td></td>
<td>a) Configure Certificate Authority Settings, on page 177</td>
</tr>
<tr>
<td></td>
<td>b) Create a CA Template, on page 178</td>
</tr>
<tr>
<td></td>
<td>c) Create a Native Supplicant Profile to be Used in Client Provisioning Policy, on page 179</td>
</tr>
<tr>
<td></td>
<td>d) Download Agent Resources from Cisco Site for Windows and MAC OS X Operating Systems, on page 180</td>
</tr>
<tr>
<td></td>
<td>e) Create Client Provisioning Policy Rules for Apple iOS, Android, and MACOSX Devices, on page 180</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication, on page 181</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Configure authorization policy rules for TLS-based authentications.</td>
</tr>
<tr>
<td></td>
<td>a) Create Authorization Profiles for Central Web Authentication and Supplicant Provisioning Flows, on page 182</td>
</tr>
<tr>
<td></td>
<td>b) Create Authorization Policy Rules, on page 182</td>
</tr>
</tbody>
</table>

When you use ECDHE-RSA based certificates, while connecting to the wireless SSID from your personal device, you
will be prompted to enter the password a second time.

---

**Add Users to the Employee User Group**

The following procedure describes how to add users to the Employee user group in the Cisco ISE identity
store. If you are using an external identity store, make sure that you have an Employee user group to which
you can add users.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose Administration &gt; Identity Management &gt; Identities &gt; Users.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click Add.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enter the user details.</td>
</tr>
</tbody>
</table>
Step 4 In the Passwords section, choose the Login Password and TACACS+ Enable Password to set the access level to a network device.

Step 5 Select Employee from the User Group drop-down list. All users who belong to the Employee user group share the same set of privileges.

Step 6 Click Submit.

---

Create a Certificate Authentication Profile for TLS-Based Authentication

To use certificates for authenticating endpoints that connect to your network, you must define a certificate authentication profile in Cisco ISE or edit the default Preloaded_Certificate_Profile. The certificate authentication profile includes the certificate field that should be used as the principal username. For example, if the username is in the Common Name field, then you can define a certificate authentication profile with the Principal Username being the Subject - Common Name, which can be verified against the identity store.

---

Create an Identity Source Sequence for TLS-Based Authentication

After you create a certificate authentication profile, you must add it to the identity source sequence so that Cisco ISE can obtain the attribute from the certificate and match it against the identity sources that you have defined in the identity source sequence.

Before you begin

Ensure that you have completed the following tasks:

- Add users to the Employee user group.
- Create a certificate authentication profile for certificate-based authentication.
Step 4  Check the **Select Certificate Authentication Profile** check box and select the certificate authentication profile that you created earlier, namely CAP.

Step 5  Move the identity source that contains your user information to the **Selected** list box in the Authentication Search List area.

You can add additional identity sources and Cisco ISE searches these data stores sequentially until a match is found.

Step 6  Click the **Treat as if the user was not found and proceed to the next store in the sequence** radio button.

Step 7  Click **Submit**.

---

**What to do next**

Configure Certificate Authority Settings, on page 177

***Configure Certificate Authority Settings***

You must configure the external CA settings if you are going to use an external CA for signing the CSRs. The external CA settings was known as the SCEP RA profile in previous releases of Cisco ISE. If you are using the Cisco ISE CA, then you do not have to explicitly configure the CA settings. You can review the Internal CA settings at Administration > System > Certificates > Internal CA Settings.

Once users’ devices receive their validated certificate, they reside on the device as described in the following table.

*Table 6: Device Certificate Location*

<table>
<thead>
<tr>
<th>Device</th>
<th>Certificate Storage Location</th>
<th>Access Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPhone/iPad</td>
<td>Standard certificate store</td>
<td>Settings &gt; General &gt; Profile</td>
</tr>
<tr>
<td>Android</td>
<td>Encrypted certificate store</td>
<td>Invisible to end users.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> Certificates can be removed using Settings &gt; Location &amp; Security &gt; Clear Storage.</td>
</tr>
<tr>
<td>Windows</td>
<td>Standard certificate store</td>
<td>Launch mmc.exe from the /cmd prompt or view in the certificate snap-in.</td>
</tr>
<tr>
<td>Mac</td>
<td>Standard certificate store</td>
<td>Application &gt; Utilities &gt; Keychain Access</td>
</tr>
</tbody>
</table>

**Before you begin**

If you are going to use an external Certificate Authority (CA) for signing the certificate signing request (CSR), then you must have the URL of the external CA.

---

**Step 1** Choose **Administration > System > Certificates > External CA Settings**.

**Step 2** Click **Add**.
Step 3  Enter a name for the external CA setting. For example, EXTERNAL_SCEP.

Step 4  Enter the external CA server URL in the URL text box.  
Click Test Connection to check if the external CA is reachable. Click the + button to enter additional CA server URLs.

Step 5  Click Submit.

What to do next
Create a CA Template, on page 178

Create a CA Template

The certificate template defines the SCEP RA profile that must be used (for the internal or external CA), Key Type, Key Size or Curve Type, Subject, Subject Alternative Name (SAN), validity period of the certificate, and the Extended Key Usage. This example assumes that you are going to use the internal Cisco ISE CA. For an external CA template, the validity period is determined by the external CA and you cannot specify it.

You can create a new CA template or edit the default certificate template, EAP_Authentication_Certificate_Template.

By default, the following CA templates are available in Cisco ISE:

- CA_SERVICE_Certificate_Template—For other network services that use the ISE CA. For example, use this certificate template while configuring ISE to issue certificates for ASA VPN users.

- EAP_Authentication_Certificate_Template—For EAP authentication.

- pxGrid_Certificate_Template—For pxGrid controller while generating the certificate from the Certificate Provisioning Portal.

Note
Certificate templates that use the ECC key type can be used only with the internal Cisco ISE CA.

Before you begin
Ensure that you have configured the CA settings.

Step 1  Choose Administration > System > CA Service > Internal CA Certificate Template.

Step 2  Enter a name for the internal CA template. For example, Internal_CA_Template.

Step 3  (Optional) Enter values for the Organizational Unit, Organization, City, State, and Country fields. 
We do not support UTF-8 characters in the certificate template fields (Organizational Unit, Organization, City, State, and Country). Certificate provisioning fails if UTF-8 characters are used in the certificate template. The username of the internal user generating the certificate is used as the Common Name of the certificate. Cisco ISE Internal CA does not support "+" or "*" characters in the Common Name field. Ensure that your username does not include "+" or "*" special characters.

Step 4  Specify the Subject Alternative Name (SAN) and the validity period of the certificate.

Step 5  Specify a Key Type. Choose RSA or ECC.
The following table lists the operating systems and versions that support ECC along with the curve types that are supported. If your devices are not running a supported operating system or on a supported version, you can use RSA-based certificates instead.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Supported Versions</th>
<th>Supported Curve Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>8 and later</td>
<td>P-256, P-384, and P-521</td>
</tr>
<tr>
<td>Android</td>
<td>4.4 and later</td>
<td>All curve types (except Android 6.0, which does not support the P-192 curve type).</td>
</tr>
</tbody>
</table>

Windows 7 and Apple iOS do not natively support ECC for EAP-TLS authentication. This release of Cisco ISE does not support the use of ECC certificates on MAC OS X devices.

If the devices in your network run an operating system that is not supported (Windows 7, MAC OS X, or Apple iOS, we recommend that you choose RSA as the Key Type.

**Step 6** (Applicable if you choose the RSA Key Type) Specify a key size. You must choose 1024 or a higher key size.

**Step 7** (Applicable only if you choose the ECC Key Type) Specify the Curve Type. The default is P-384.

**Step 8** Choose ISE Internal CA as the SCEP RA Profile.

**Step 9** Enter the validity period in days. The default is 730 days. Valid range is between 1 and 730.

**Step 10** Specify the Extended Key Usage. Check the **Client Authentication** check box if you want the certificate to be used for client authentication. Check the **Server Authentication** check box if you want the certificate to be used for server authentication.

**Step 11** Click Submit.

The internal CA certificate template is created and will be used by the client provisioning policy.

**What to do next**

Create a Native Supplicant Profile to be Used in Client Provisioning Policy, on page 179

**Create a Native Supplicant Profile to be Used in Client Provisioning Policy**

You can create native supplicant profiles to enable users to bring personal devices to your Corporate network. Cisco ISE uses different policy rules for different operating systems. Each client provisioning policy rule contains a native supplicant profile, which specifies which provisioning wizard is to be used for which operating system.

**Before you begin**

- Configure the CA certificate template in Cisco ISE.
- Open up TCP port 8905 and UDP port 8905 to enable Cisco NAC Agent, Cisco NAC Web Agent, and supplicant provisioning wizard installation. For more information on port usage, see the "Cisco ISE Appliance Ports Reference" appendix in the Cisco Identity Services Engine Hardware Installation Guide.
Step 1  Choose Policy > Policy Elements > Results > Client Provisioning > Resources.
Step 2  Choose Add > Native Supplicant Profile.
Step 3  Enter a name for the native supplicant profile. For example, EAP_TLS_INTERNAL.
Step 4  Choose ALL from the Operating System drop-down list.

Note  The MAC OS version 10.10 user should manually connect to the provisioned SSID for dual-SSID PEAP flow.

Step 5  Check the Wired or Wireless check box.
Step 6  Choose TLS from the Allowed Protocol drop-down list.
Step 7  Choose the CA certificate template that you created earlier.
Step 8  Click Submit.

What to do next
Download Agent Resources from Cisco Site for Windows and MAC OS X Operating Systems, on page 180

Download Agent Resources from Cisco Site for Windows and MAC OS X Operating Systems

For Windows and MAC OS X operating systems, you must download the remote resources from the Cisco site.

Before you begin
Ensure that you are able to access the appropriate remote location to download client provisioning resources to Cisco ISE, by verifying that the proxy settings for your network are correctly configured.

Step 1  Choose Policy > Policy Elements > Resources > Client Provisioning > Resources.
Step 2  Choose Add > Agent resources from Cisco site.
Step 3  Check the check boxes next to the Windows and MAC OS X packages. Be sure to include the latest versions.
Step 4  Click Save.

What to do next
Create Client Provisioning Policy Rules for Apple iOS, Android, and MACOSX Devices, on page 180

Create Client Provisioning Policy Rules for Apple iOS, Android, and MACOSX Devices

Client provisioning resource policies determine which users receive which version (or versions) of resources (agents, agent compliance modules, and agent customization packages/profiles) from Cisco ISE upon login and user session initiation.

When you download the agent compliance module, it always overwrites the existing one, if any, available in the system.

To enable employees to bring iOS, Android, MACOSX devices, you must create policy rules for each of these devices on the Client Provisioning Policy page.
Before you begin

You must have configured the required native supplicant profiles and downloaded the required agents from the Client Provisioning Policy pages.

Step 1 Choose Policy > Client Provisioning.
Step 2 Create client provisioning policy rules for Apple iOS, Android, and MACOSX devices.
Step 3 Click Save.

What to do next

Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication, on page 181

Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication

This task shows how to update the Dot1X authentication policy rule for TLS-based authentications.

Before you begin

Ensure that you have the certificate authentication profile created for TLS-based authentication.

Step 1 Choose Policy > Policy Sets.
Step 2 Click the arrow icon ➔ from the View column to open the Set view screen and view, manage, and update the authentication policy.

The default rule-based authentication policy includes a rule for Dot1X authentication.

Step 3 To edit the conditions for the Dot1X authentication policy rule, hover over the cell in the Conditions column and click The Conditions Studio opens.

Step 4 From the Actions column in the Dot1X policy rule, click the cog icon and then from the drop-down menu, insert a new policy set by selecting any of the insert or duplicate options, as necessary.

A new row appears in the Policy Sets table.

Step 5 Enter a name for the rule. For example, eap-tls.
Step 6 From the Conditions column, click the (+) symbol.
Step 7 Create the required conditions in the Conditions Studio Page. In the Editor section, click the Click To Add an Attribute text box, and select the required Dictionary and Attribute (for example, Network Access:UserName Equals User1).

You can drag and drop a Library condition to the Click To Add An Attribute text box.

Step 8 Click Use.
Step 9 Leave the default rule as is.
Step 10 Click Save.
What to do next
Create Authorization Profiles for Central Web Authentication and Supplicant Provisioning Flows, on page 182

Create Authorization Profiles for Central Web Authentication and Supplicant Provisioning Flows
You must define authorization profiles to determine the access that must be granted to the user after the certificate-based authentication is successful.

Before you begin
Ensure that you have configured the required access control lists (ACLs) on the wireless LAN controller (WLC). Refer to the TrustSec How-To Guide: Using Certificates for Differentiated Access for information on how to create the ACLs on the WLC.
This example assumes that you have created the following ACLs on the WLC.
• NSP-ACL - For native supplicant provisioning
• BLACKHOLE - For restricting access to blacklisted devices
• NSP-ACL-Google - For provisioning Android devices

Step 1 Choose Policy > Policy Elements > Results > Authorization > Authorization Profiles.
Step 2 Click Add to create a new authorization profile.
Step 3 Enter a name for the authorization profile.
Step 4 From the Access Type drop-down list, choose ACCESS_ACCEPT.
Step 5 Click Add to add the authorization profiles for central web authentication, central web authentication for Google Play, native supplicant provisioning, and native supplicant provisioning for Google.
Step 6 Click Save.

What to do next
Create Authorization Policy Rules, on page 182

Create Authorization Policy Rules
Cisco ISE evaluates the authorization policy rules and grants the user access to the network resources based on the authorization profile specified in the policy rule.

Before you begin
Ensure that you have created the required authorization profiles.

Step 1 Choose Policy > Policy Sets, and expand the policy set to view the authorization policy rules.
Step 2 Insert additional policy rules above the default rule.
Step 3  Click Save.

CA Service Policy Reference

This section provides reference information for the authorization and client provisioning policy rules that you must create before you can enable the Cisco ISE CA service.

Client Provisioning Policy Rules for Certificate Services

This section lists the client provisioning policy rules that you must create while using the Cisco ISE certificate services. The following table provides the details.

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Identity Groups</th>
<th>Operating Systems</th>
<th>Other Conditions</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS</td>
<td>Any</td>
<td>Apple iOS All</td>
<td>Condition(s)</td>
<td>EAP_TLS_INTERNAL (the native supplicant profile that you created earlier). If you are using an external CA, select the native supplicant profile that you have created for the external CA.</td>
</tr>
<tr>
<td>Android</td>
<td>Any</td>
<td>Android</td>
<td>Condition(s)</td>
<td>EAP_TLS_INTERNAL (the native supplicant profile that you created earlier). If you are using an external CA, select the native supplicant profile that you have created for the external CA.</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Identity Groups</td>
<td>Operating Systems</td>
<td>Other Conditions</td>
<td>Results</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------</td>
<td>-------------------</td>
<td>-----------------</td>
<td>---------</td>
</tr>
<tr>
<td>MACOSX</td>
<td>Any</td>
<td>MACOSX</td>
<td>Condition(s)</td>
<td>Under the Native Supplicant Configuration, specify the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1. Config Wizard: Select the MACOSX supplicant wizard that you downloaded from the Cisco site.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2. Wizard Profile: Choose the EAP_TTLS_INTERNAL native supplicant profile that you created earlier. If you are using an external CA, select the native supplicant profile that you have created for the external CA.</td>
</tr>
</tbody>
</table>

### Authorization Profiles for Certificate Services

This section lists the authorization profiles that you must create for enabling certificate-based authentication in Cisco ISE. You must have already created the ACLs (NSP-ACL and NSP-ACL-Google) on the wireless LAN controller (WLC).

- **CWA** - This profile is for devices that go through the central web authentication flow. Check the **Web Authentication** check box, choose Centralized from the drop-down list, and enter NSP-ACL in the ACL text box.

- **CWA_GooglePlay** - This profile is for Android devices that go through the central web authentication flow. This profile enables Android devices to access Google Play Store and download the Cisco Network Setup Assistant. Check the **Web Authentication** check box, choose Centralized from the drop-down list, and enter NSP-ACL-Google in the ACL text box.

- **NSP** - This profile is for non-Android devices that go through the supplicant provisioning flow. Check the **Web Authentication** check box, choose Supplicant Provisioning from the drop-down list, and enter NSP-ACL in the ACL text box.

- **NSP-Google** - This profile is for Android devices that go through the supplicant provisioning flow. Check the **Web Authentication** check box, choose Supplicant Provisioning from the drop-down list, and enter NSP-ACL-Google in the ACL text box.
Review the default Blackhole_Wireless_Access authorization profile. The Advanced Attributes Settings should be:

- Cisco:cisco-av-pair = url-redirect-acl=BLACKHOLE

**Authorization Policy Rules for Certificate Services**

This section lists the authorization policy rules that you must create while enabling the Cisco ISE CA service.

- Corporate Assets - This rule is for corporate devices that connect to the corporate wireless SSID using 802.1X and MSCHAPV2 protocol.
- Android_SingleSSID - This rule is for Android devices that access the Google Play Store to download the Cisco Network Setup Assistant for provisioning. This rule is specific to single SSID setup.
- Android_DualSSID - This rule is for Android devices that access the Google Play Store to download the Cisco Network Setup Assistant for provisioning. This rule is specific to dual SSID setup.
- CWA - This rule is for devices that go through the central web authentication flow.
- NSP - This rule is for devices that go through the native supplicant provisioning flow using a certificate for EAP-TLS authentication.
- EAP-TLS - This rule is for devices that have completed the supplicant provisioning flow and are provisioned with a certificate. They will be given access to the network.

The following table lists the attributes and values that you must choose while configuring authorization policy rules for the Cisco ISE CA service. This example assumes that you have the corresponding authorization profiles configured in Cisco ISE as well.

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Conditions</th>
<th>Permissions (authorization profiles to be applied)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate Assets</td>
<td>Corp_Assets AND (Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)</td>
<td>PermitAccess</td>
</tr>
<tr>
<td>Android_DualSSID</td>
<td>(Wireless MAB AND Session:Device-OS EQUALS Android)</td>
<td>CWA_GooglePlay</td>
</tr>
<tr>
<td>CWA</td>
<td>Wireless_MAB</td>
<td>CWA</td>
</tr>
<tr>
<td>NSP</td>
<td>(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)</td>
<td>NSP</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS x509_PKI)</td>
<td>PermitAccess</td>
</tr>
</tbody>
</table>
ISE CA Issues Certificates to ASA VPN Users

ISE CA issues certificates to client machines connecting over ASA VPN. Using this feature, you can automatically provision certificates to end devices that connect over ASA VPN.

Cisco ISE uses the Simple Certificate Enrollment Protocol (SCEP) for enrollment and to provision certificates to the client machines. The AnyConnect client sends the SCEP request to the ASA over an HTTPS connection. The ASA evaluates the request and enforces policies before it relays the request to Cisco ISE over an HTTP connection established between Cisco ISE and ASA. The response from the Cisco ISE CA is relayed back to the client. The ASA cannot read the contents of the SCEP message and functions as a proxy for the Cisco ISE CA. The Cisco ISE CA decrypts the SCEP message from the client and sends the response in an encrypted form.

The ISE CA SCEP URL is http://<IP Address or FQDN of ISE CA server>:9090/auth/caservice/pkiclient.exe. If you are using FQDN of the ISE node, the DNS server connected to ASA must be able to resolve the FQDN.

You can configure certificate renewal before expiration in the AnyConnect Client profile. If the certificate has already expired, the renewal flow is similar to a new enrollment.

Supported versions include:
- Cisco ASA 5500 Series Adaptive Security Appliances that run software version 8.x
- Cisco AnyConnect VPN version 2.4 or later

VPN Connection Certificate Provisioning Flow

**Figure 8: Certificate Provisioning for ASA VPN Users**

1. The user initiates a VPN connection.
2. The AnyConnect client scans the client machine and sends the attributes such as the unique device identifier (for example, IMEI) to the ASA.

3. The ASA requests certificate-based authentication from the client. The authentication fails because there is no certificate.

4. The ASA proceeds to primary user authentication (AAA) using the username/password and passes the information to the authentication server (ISE).
   1. If authentication fails, the connection is terminated immediately.
   2. If authentication passes, limited access is granted. You can configure dynamic access policies (DAP) for client machines that request a certificate using the aaa.cisco.sceprequired attribute. You can set the value for this attribute to “true” and apply ACLs and web ACLs.

5. The VPN connection is established after the relevant policies and ACLs are applied. The client starts key generation for SCEP only after AAA authentication succeeds and the VPN connection is established.

6. The client starts the SCEP enrollment and sends SCEP requests to ASA over HTTP.

7. ASA looks up the session information of the request and relays the request to ISE CA, if the session is allowed for enrollment.

8. ASA relays the response from ISE CA back to the client.

9. If enrollment succeeds, the client presents a configurable message to the user and disconnects the VPN session.

10. The user can again authenticate using the certificate and a normal VPN connection is established.

**Configure Cisco ISE CA to Issue Certificates to ASA VPN Users**

You must perform the following configurations on Cisco ISE and ASA to provision certificates to ASA VPN users.

**Before you begin**

- Ensure that the VPN user account is present in Cisco ISE internal or external identity source.
- Ensure that the ASA and the Cisco ISE Policy Service Nodes are synchronized using the same NTP server.

---

**Step 1**
Define the ASA as a network access device in Cisco ISE. See [Create a Network Device Definition in Cisco ISE](#) on page 188 for information on how to add ASA as a network device.

**Step 2**
Configure Group Policy in ASA, on page 188.

**Step 3**
Configure AnyConnect Connection Profile for SCEP Enrollment, on page 188.

**Step 4**
Configure a VPN Client Profile in ASDM, on page 189.

**Step 5**
Import Cisco ISE CA Certificates into ASA.
Create a Network Device Definition in Cisco ISE

You can create a network device definition in Cisco ISE and use the default network device definition when there is no network device definition in Cisco ISE.

You can also create the network device definition in the Work Centers > Device Administration > Network Resources > Network Devices page.

---

**Step 1** Choose Administration > Network Resources > Network Devices.

**Step 2** Click Add.

**Step 3** Complete all mandatory fields.

**Step 4** Check the RADIUS Authentication Settings check box to configure the RADIUS protocol for authentication.

**Step 5** Check the TACACS Authentication Settings check box to configure the TACACS protocol for authentication.

**Step 6** (Optional) Check the SNMP Settings check box to configure the Simple Network Management Protocol for the Profiling service to collect device information.

**Step 7** (Optional) Check the Advanced Trustsec Settings check box to configure a Trustsec-enabled device.

**Step 8** Click Submit.

---

Configure Group Policy in ASA

Configure a group policy in ASA to define the ISE CA URL for AnyConnect to forward the SCEP enrollment request.

**Step 1** Log in to Cisco ASA ASDM.

**Step 2** From the Remote Access VPN navigation pane on the left, click Group Policies.

**Step 3** Click Add to create a group policy.

**Step 4** Enter a name for the group policy. For example, ISE_CA_SCEP.

**Step 5** In the SCEP forwarding URL field, uncheck the Inherit check box and enter the ISE SCEP URL with port number.

If you are using the FQDN of the ISE node, the DNS server connected to ASA must be able to resolve the FQDN of the ISE node.

**Example:**

**Step 6** Click OK to save the group policy.

---

Configure AnyConnect Connection Profile for SCEP Enrollment

Configure an AnyConnect connection profile in ASA to specify the ISE CA server, authentication method, and ISE CA SCEP URL.

**Step 1** Log in to Cisco ASA ASDM.

**Step 2** From the Remote Access VPN navigation pane on the left, click AnyConnect Connection Profiles.

**Step 3** Click Add to create a connection profile.
Step 4 Enter a name for the connection profile. For example, Cert-Group.
Step 5 (Optional) Enter a description for the connection profile in the Aliases field. For example, SCEP-Call-ASA.
Step 6 In the Authentication area, specify the following:
   • Method—Click the Both radio button
   • AAA Server Group—Click Manage and choose your ISE server
Step 7 In the Client Address Assignment area, select the DHCP server and client address pools to use.
Step 8 In the Default Group Policy area, click Manage and select the Group Policy that you have created with the ISE SCEP URL and port number.
   Example:
   For example, ISE_CA_SCEP.
Step 9 Choose Advanced > General and check the Enable Simple Certificate Enrollment Protocol check box for this connection profile.
Step 10 Click OK.
   Your AnyConnect connection profile is created.

What to do next

Configure a VPN Client Profile in ASDM

Configure a VPN client profile in AnyConnect for SCEP enrollment.

Step 1 Log in to Cisco ASA ASDM.
Step 2 From the Remote Access VPN navigation pane on the left, click AnyConnect Client Profile.
Step 3 Select the client profile that you want to use and click Edit.
Step 4 Click Certificate Enrollment from the Profile navigation pane on the left.
Step 5 Check the Certificate Enrollment check box.
Step 6 Enter the values in the following fields:
   • Certificate Expiration Threshold—The number of days before the certificate expiration date that AnyConnect warns users their certificate is going to expire (not supported when SCEP is enabled). The default is zero (no warning displayed). The range of values is zero to 180 days.
   • Automatic SCEP Host—Enter the host name and connection profile (tunnel group) of the ASA that has SCEP certificate retrieval configured. Enter a Fully Qualified Domain Name (FQDN) or a connection profile name of the ASA. For example, the hostname asa.cisco.com and the connection profile name Cert_Group.
   • CA URL—Identifies the SCEP CA server. Enter the FQDN or IP Address of the ISE server. For example, http://ise01.cisco.com:9090/auth/caservice/pkiclient.exe.
Step 7 Enter values for the Certificate Contents that define how the client requests the contents of the certificate.
Step 8 Click OK.
   The AnyConnect client profile is created. Refer to the Cisco AnyConnect Secure Mobility Client for your version of AnyConnect for additional information.
Import Cisco ISE CA Certificates into ASA

Export the Cisco ISE internal CA certificates. Go to Administration > System > Certificates > Trusted certificates. Check the check boxes next to Certificate Services Node CA and Certificate Services Root CA certificates and export them.

Step 1: Log in to Cisco ASA ASDM.
Step 2: From the Remote Access VPN navigation pane on the left, choose Certificate Management > CA Certificates.
Step 3: Click Add and select the Cisco ISE internal CA certificates to import them into ASA.

Revoke an Endpoint Certificate

If you need to revoke a certificate issued to an employee's personal device, you can revoke it from the Endpoint Certificates page. For example, if an employee's device has been stolen or lost, you can log in to the Cisco ISE Admin portal and revoke the certificate issued to that device from the Endpoint Certificates page. You can filter the data on this page based on the Friendly Name, Device Unique Id, or Serial Number. If a PSN (sub CA) is compromised, you can revoke all certificates issued by that PSN by filtering on the Issued By field from the Endpoint Certificates page.

When you revoke a certificate issued to an employee, if there is an active session (authenticated using that certificate), the session is terminated immediately. Revoking a certificate ensures that unauthorized users do not have any access to resources as soon as the certificate is revoked.

Step 1: Choose Administration > System > CA Service > Endpoint Certificates.
Step 2: Check the check box next to the endpoint certificate that you want to revoke and click Revoke.
You can search for the certificate based on the Friendly Name and Device Type.
Step 3: Enter the reason for revoking the certificate.
Step 4: Click Yes.

OCSP Services

The Online Certificate Status Protocol (OCSP) is a protocol that is used for checking the status of x.509 digital certificates. This protocol is an alternative to the Certificate Revocation List (CRL) and addresses issues that result in handling CRLs.

Cisco ISE has the capability to communicate with OCSP servers over HTTP to validate the status of certificates in authentications. The OCSP configuration is configured in a reusable configuration object that can be referenced from any certificate authority (CA) certificate that is configured in Cisco ISE.
You can configure CRL and/or OCSP verification per CA. If both are selected, then Cisco ISE first performs verification over OCSP. If a communication problem is detected with both the primary and secondary OCSP servers, or if an unknown status is returned for a given certificate, Cisco ISE switches to checking the CRL.

**Cisco ISE CA Service Online Certificate Status Protocol Responder**

The Cisco ISE CA OCSP responder is a server that communicates with OCSP clients. The OCSP clients for the Cisco ISE CA include the internal Cisco ISE OCSP client and OCSP clients on the Adaptive Security Appliance (ASA). The OCSP clients should communicate with the OCSP responder using the OCSP request/response structure defined in RFC 2560, 5019.

The Cisco ISE CA issues a certificate to the OCSP responder. The OCSP responder listens on port 2560 for any incoming requests. This port is configured to allow only OCSP traffic.

The OCSP responder accepts a request that follows the structure defined in RFC 2560, 5019. Nonce extension is supported in the OCSP request. The OCSP responder obtains the status of the certificate and creates an OCSP response and signs it. The OCSP response is not cached on the OCSP responder, although you can cache the OCSP response on the client for a maximum period of 24 hours. The OCSP client should validate the signature in the OCSP response.

The self-signed CA certificate (or the intermediate CA certificate if ISE acts as an intermediate CA of an external CA) on the PAN issues the OCSP responder certificate. This CA certificate on the PAN issues the OCSP certificates on the PAN and PSNs. This self-signed CA certificate is also the root certificate for the entire deployment. All the OCSP certificates across the deployment are placed in the Trusted Certificates Store for ISE to validate any response signed using these certificates.

**OCSP Certificate Status Values**

OCSP services return the following values for a given certificate request:

- **Good**—Indicates a positive response to the status inquiry. It means that the certificate is not revoked, and the state is good only until the next time interval (time to live) value.

- **Revoked**—The certificate was revoked.

- **Unknown**—The certificate status is unknown. OCSP service returns this value if the certificate was not issued by the CA of this OCSP responder.

- **Error**—No response was received for the OCSP request.

**OCSP High Availability**

Cisco ISE has the capability to configure up to two OCSP servers per CA, and they are called primary and secondary OCSP servers. Each OCSP server configuration contains the following parameters:

- **URL**—The OCSP server URL.

- **Nonce**—A random number that is sent in the request. This option ensures that old communications cannot be reused in replay attacks.

- **Validate response**—Cisco ISE validates the response signature that is received from the OCSP server.
In case of timeout (which is 5 seconds), when Cisco ISE communicates with the primary OCSP server, it switches to the secondary OCSP server.

Cisco ISE uses the secondary OCSP server for a configurable amount of time before attempting to use the primary server again.

**OCSP Failures**

The three general OCSP failure scenarios are as follows:

- Failed OCSP cache or OCSP client side (Cisco ISE) failures.
- Failed OCSP responder scenarios, for example:
  - The first primary OCSP responder not responding, and the secondary OCSP responder responding to the Cisco ISE OCSP request.
  - Errors or responses not received from Cisco ISE OCSP requests.
  - An OCSP responder may not provide a response to the Cisco ISE OCSP request or it may return an OCSP Response Status as not successful. OCSP Response Status values can be as follows:
    - tryLater
    - signRequired
    - unauthorized
    - internalError
    - malformedRequest
  - There are many date-time checks, signature validity checks and so on, in the OCSP request. For more details, refer to [RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP](https://tools.ietf.org/html/rfc2560) which describes all the possible states, including the error states.

- Failed OCSP reports

**Add OCSP Client Profiles**

You can use the OCSP Client Profile page to add new OCSP client profiles to Cisco ISE.

**Before you begin**

If the Certificate Authority (CA) is running the OCSP service on a nonstandard port (other than 80 or 443), you must configure ACLs on the switch to allow for communication between Cisco ISE and the CA on that port. For example:

```
permit tcp <source ip> <destination ip> eq <OCSP port number>
```

**Step 1** Choose **Administration > System > Certificates > Certificate Management > OCSP Client Profile**.

**Step 2** Enter the values to add an OCSP Client Profile.

**Step 3** Click **Submit**.
OCSP Statistics Counters

Cisco ISE uses OCSP counters to log and monitor the data and health of the OCSP servers. Logging occurs every five minutes. Cisco ISE sends a syslog message to the Monitoring node and it is preserved in the local store. The local store contains data from the previous five minutes. After Cisco ISE sends the syslog message, the counters are recalculated for the next interval. This means, after five minutes, a new five-minute window interval starts again.

The following table lists the OCSP syslog messages and their descriptions.

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OCSPPrimaryNot Responsive Count</td>
<td>The number of nonresponsive primary requests</td>
</tr>
<tr>
<td>OCSPSecondaryNot Responsive Count</td>
<td>The number of nonresponsive secondary requests</td>
</tr>
<tr>
<td>OCSPPrimaryCerts Good Count</td>
<td>The number of ‘good’ certificates that are returned for a given CA using the primary OCSP server</td>
</tr>
<tr>
<td>OCSPSecondaryCerts Good Count</td>
<td>The number of ‘good’ statuses that are returned for a given CA using the primary OCSP server</td>
</tr>
<tr>
<td>OCSPPrimaryCerts Revoked Count</td>
<td>The number of ‘revoked’ statuses that are returned for a given CA using the primary OCSP server</td>
</tr>
<tr>
<td>OCSPSecondaryCerts Revoked Count</td>
<td>The number of ‘revoked’ statuses that are returned for a given CA using the secondary OCSP server</td>
</tr>
<tr>
<td>OCSPPrimaryCerts Unknown Count</td>
<td>The number of ‘Unknown’ statuses that are returned for a given CA using the primary OCSP server</td>
</tr>
<tr>
<td>OCSPSecondaryCerts Unknown Count</td>
<td>The number of ‘Unknown’ statuses that are returned for a given CA using the secondary OCSP server</td>
</tr>
<tr>
<td>OCSPPrimaryCerts Found Count</td>
<td>The number of certificates that were found in cache from a primary origin</td>
</tr>
<tr>
<td>OCSPSecondaryCerts Found Count</td>
<td>The number of certificates that were found in cache from a secondary origin</td>
</tr>
<tr>
<td>ClearCacheInvoked Count</td>
<td>How many times clear cache was triggered since the interval</td>
</tr>
<tr>
<td>OCSP Certs Cleaned Up Count</td>
<td>How many cached entries were cleaned since the interval</td>
</tr>
<tr>
<td>NumOfCerts Found In Cache</td>
<td>Number of the fulfilled requests from the cache</td>
</tr>
<tr>
<td>OCSP Cache Certs Count</td>
<td>Number of certificates that were found in the OCSP cache</td>
</tr>
</tbody>
</table>
CHAPTER 9

Control Device Administration Using TACACS+

• Device Administration, on page 195
• Device Administration Work Center, on page 197
• Data Migration from Cisco Secure ACS to Cisco ISE, on page 197
• Device Administration Deployment Settings, on page 197
• Device Admin Policy Sets, on page 198
• TACACS+ Authentication Settings and Shared Secret, on page 198
• Device Administration - Authorization Policy Results, on page 200
• Create Device Administration Policy Sets, on page 206
• Monitor Device Administration Activity, on page 207
• Configure Global TACACS+ Settings, on page 208

Device Administration

There are two types of administrators for device administration:

• Device Administrator

• ISE Administrator

The device administrator is the user who logs into the network devices such as switches, wireless access points, routers, and gateways, (normally through SSH), in order to perform the configuration and maintenance of the administered devices. The ISE administrator logs into ISE to configure and coordinate the devices that a device administrator logs in to.

The ISE administrator is the intended reader of this document, who logs into ISE to configure the settings that control the operations of the device administrator. The ISE administrator uses the device administration features (Work centers > Device Administration) to control and audit the configuration of the network devices. A device can be configured to query the ISE server using the Terminal Access Controller Access-Control System (TACACS) security protocol. The ISE Monitoring node provides enhanced reports related to device administration. An ISE administrator can perform the following tasks:

• Configure network devices with the TACACS+ details (shared secret).

• Add device administrators as internal users and set their enable passwords as needed.

• Create policy sets that allow TACACS results, such as command sets and shell profiles, to be selected in authorization policy rules in a device administration access service.
• Configure the TACACS server in ISE to allow device administrators to access devices based on the policy sets.

The device administrator performs the task of setting up a device to communicate with the ISE server. When a device administrator logs on to a device, the device queries the ISE server, which in turn queries an internal or external identity store, to validate the details of the device administrator. When the validation is done by the ISE server, the device informs the ISE server of the final outcome of each session or command authorization operation for accounting and auditing purposes.

An ISE administrator can manage device administration using TACACS and Cisco ISE 2.1. The configuration related to device administration can also be migrated from a Cisco Secure Access Control System (ACS) server, versions 5.5, 5.6, 5.7 and 5.8. Prior versions need to be upgraded to 5.5 or 5.6 before migration.

**Note**
You should enable the device admin services in the Work Centers > Device Administration > Overview > Deployment page.

**Note**
Cisco ISE requires a Device Administration license to use the TACACS+ service on top of an existing Base or Mobility license. The Device Administration license is a perpetual license. If you are upgrading from an earlier release to Cisco ISE, Release 2.0 and later, and would like to enable the TACACS+ service, you must order the Device Administration license as a separate add-on license. You need one Device Administration license for the entire ISE deployment.

ISE Community Resource
For information about device administration attributes, see ISE Device Administration Attributes.
For information about TACACS+ configuration for Wireless LAN controllers, IOS network devices, Cisco NX-OS network devices, and network devices, see ISE Device Administration (TACACS+).

### Access the Command-Line Interface to Change the Enable Password

To change Enable password, perform the following steps:

**Before you begin**

Some commands are assigned to privileged mode. Therefore, they can only be executed when the device administrator has authenticated into this mode.

The device sends a special enable authentication type when the device administrator attempts to enter the privileged mode. Cisco ISE supports a separate enable password to validate this special enable authentication type. The separate enable password is used when the device administrator is authenticated with internal identity stores. For authentication with external identity stores, the same password is used as for regular login.

**Step 1**
Log in to the switch.

**Step 2**
Press Enter to display the following prompt:

Switch>
Step 3  Execute the following commands to configure the Enable password.

```bash
Switch> enable
Password: (Press Enter to leave the password blank.)
Enter Old Password: (Enter the old password.)
Enter New Password: (Enter the new password.)
Enter New Password Confirmation: (Confirm the new password.)
```

**Note**  If password lifetime is configured for the Login password and Enable password, the user account will be disabled if the passwords are not changed within the specified time period. If Cisco ISE is configured as TACACS+ server and the Enable Bypass option is configured on the network device, you cannot change the Enable password from the CLI (via telnet). Choose Administration > Identity Management > Identities > Users to change the Enable password for internal users.

---

**Device Administration Work Center**

The Work Center menu contains all the device administration pages, which acts as a single start point for ISE administrators. However, pages that are not specific to device administration such as Users, User Identity Groups, Network Devices, Default Network Devices, Network Device Groups, Authentication and Authorization Conditions, can still be accessed from their original menu options, such as Administration. The Work Centers option is available only if the correct TACACS+ license(s) are obtained and installed.

The Device Administration Menu contains the following menu options: Overview, Identities, User Identity Groups, Ext ID Stores, Network Resources, Network Device Groups, Policy Elements, Device Admin Policy Sets, Reports, and Settings.

**Data Migration from Cisco Secure ACS to Cisco ISE**

You can use the migration tool to import data from ACS 5.5 and later, and set default TACACS+ secret for all network devices. Navigate to Work Centers > Device Administration > Overview and in the Prepare section, click Download Software Webpage to download the migration tool. Save the tool to your PC, and from the migTool folder, run the migration.bat file to start the migration process. For complete information related to the migration, refer to the Migration Guide for your version of ISE.

**Device Administration Deployment Settings**

The Device Administration Deployment page (Work Centers > Device Administration > Overview > Deployment) allows ISE administrators to centrally view the device administration system without referring to each node in the deployment section.

The Device Administration Deployment page lists the PSNs in your deployment. This simplifies the task of enabling the device admin service individually in each PSN in your deployment. You can collectively enable the device admin service for many PSNs by selecting an option below:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>By default, the device administration service is disabled for all nodes.</td>
</tr>
</tbody>
</table>
### Device Admin Policy Sets

The Device Admin Policy Sets page (Work Centers > Device Administration > Device Admin Policy Sets) contains the list of policy sets that an ISE administrator manages to control the authentication and authorization of TACACS+ Device administrators. Each policy can be in one of two modes: Regular and Proxy Sequence.

A Regular policy set comprises an authentication rule table and an authorization rule table. The authentication rule table contains a set of rules to select actions required to authenticate a network device.

The authorization rule table contains a set of rules to select the specific authorization results required to implement the authorization business model. Each authorization rule consists of one or more conditions that must be matched for the rule to be engaged, and a set of command sets, and/or a shell profile, which are selected to control the authorization process. Each rule table has an exception policy that can be used to override the rules for specific circumstances, often the exception table is used for temporary situations.

A Proxy Sequence policy set contains a single selected proxy sequence. If the policy set is in this mode then the remote proxy server(s) are used to process the requests (although local accounting may be configured by the Proxy Sequence).

### TACACS+ Authentication Settings and Shared Secret

The following table describes the fields on the Network Devices page, which you can use to configure TACACS+ authentication settings for a network device. The navigation path is:

- (For Network Devices) Work Centers > Device Administration > Network Resources > Network Devices > Add > TACACS Authentication Settings.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Policy Service Nodes</td>
<td>Enables the device administration service in all PSNs. With this option, new PSNs are automatically enabled for device admin when they are added.</td>
</tr>
<tr>
<td>Specific Nodes</td>
<td>Displays the ISE Nodes section that lists all the PSNs in your deployment. You can select the required nodes that necessitate the device admin service to be enabled.</td>
</tr>
</tbody>
</table>

If the deployment is not licensed for TACACS+, the above options are disabled.

The TACACS Ports field allows you to enter a maximum of four TCP ports, which are comma-separated and port values range from 1 to 65535. Cisco ISE nodes and their interfaces listen for TACACS+ requests on the specified ports and you must ensure that the specified ports are not used by other services. The default TACACS+ port value is 49.

When you click Save, the changes are synchronized with the nodes specified in the Administration > System > Deployment Listing page.
• (For Default Devices) Work Centers > Device Administration > Network Resources > Default Devices > TACACS Authentication Settings. You can refer to the Default Network Device Definition in Cisco ISE section for more information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared Secret</td>
<td>A string of text assigned to a network device when TACACS+ protocol is enabled. A user must enter the text before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret. This is not a mandatory field.</td>
</tr>
<tr>
<td>Retired Shared Secret is Active</td>
<td>Displayed when the retirement period is active.</td>
</tr>
<tr>
<td>Retire</td>
<td>Retires an existing shared secret instead of ending it. When you click Retire, a message box is displayed. You can either click Yes or No.</td>
</tr>
<tr>
<td>Remaining Retired Period</td>
<td>(Available only if you select Yes in the above message box) Displays the default value specified in the following navigation path: Work Centers &gt; Device Administration &gt; Settings &gt; Connection Settings &gt; Default Shared Secret Retirement Period. You can change the default values. This allows a new shared secret to be entered and the old shared secret will remain active for the specified number of days.</td>
</tr>
<tr>
<td>End</td>
<td>(Available only if you select Yes in the above message box) Ends the retirement period and terminates the old shared secret.</td>
</tr>
<tr>
<td>Enable Single Connect Mode</td>
<td>Check to use a single TCP connection for all TACACS+ communication with the network device. Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Legacy Cisco Devices</td>
</tr>
<tr>
<td></td>
<td>• Or, TACACS+ Draft Compliance Single Connect Support. If you disable Single Connect Mode, ISE uses a new TCP connection for every TACACS+ request.</td>
</tr>
</tbody>
</table>

In summary, you can

• Retire the old shared secret by specifying the retirement period as number of days (Range is 1 to 99) and at the same time set a new shared secret.

• Use the old and new shared secrets during the retirement period.

• Extend the retirement period before it expires.

• Use the old shared secret only until the end of the retirement period.
Device Administration - Authorization Policy Results

ISE administrators can use the TACACS+ command sets and TACACS+ profiles (policy results) to exercise control over the privileges and commands that are granted to a device administrator. The policy works in conjunction with the network devices and thereby prevents accidental or malicious configuration changes that may be done. In the event such changes occur, you can use the device administration audit reports to track the device administrator who has executed a particular command.

Related Topics
- TACACS+ Command Sets, on page 200
- TACACS+ Profile, on page 202

Allowed Protocols in FIPS and Non-FIPS Modes for TACACS+ Device Administration

There are many allowed authentication protocol services that Cisco ISE offers for creating the policy results. However, authentication protocol services such as PAP/ASCII, CHAP, and MS-CHAPv1, which are applicable to the TACACS+ protocol, are disabled on FIPS-enabled Cisco ISE appliances for RADIUS. As a result, these protocols cannot be enabled in the Policy > Policy Elements > Results > Allowed Protocols page to administer devices, when using a FIPS-enabled (Administration > System Settings > FIPS Mode) Cisco ISE appliance.

Consequently, to configure PAP/ASCII, CHAP, and MS-CHAPv1 protocols in your device administration policy results, for both FIPS and non-FIPS modes, you must navigate to the Work Centers > Device Administration > Policy Elements > Results > Allowed Protocols page. Only the Default Device Admin allowed protocols setting may be used when FIPS mode is enabled. This option is not allowed in RADIUS.

TACACS+ Command Sets

Command sets enforce the specified list of commands that can be executed by a device administrator. When a device administrator issues operational commands on a network device, ISE is queried to determine whether the administrator is authorized to issue these commands. This is also referred to as command authorization.

Wildcards and Regex in Command Sets

A command line comprises the command and zero or more arguments. When Cisco ISE receives a command line (request), it handles the command and its arguments in different ways:

- It matches the command in the request with the commands specified in the command set list using the wildcard matching paradigm.

  Example: Sh?? or S*
It matches the arguments in the request with the arguments specified in the command set list using regular expressions (regex) matching paradigm.

Example: Show interface[1-4] port[1-9]:tty*

Command Line and Command Set List Match

To match a requested command line to a command set list containing wildcards and regex:

1. Iterate over a command set list to detect matching commands.
   
   Wildcard matching permits:
   
   • Case insensitivity
   
   • Any character in the command in the command set may be "?", which matches any individual character that must exist in the requested command
   
   • Any character in the command in the command set may be "*", which matches zero or more characters in the requested command
   
   Examples:

<table>
<thead>
<tr>
<th>Request</th>
<th>Command Set</th>
<th>Matches</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>show</td>
<td>show</td>
<td>Y</td>
<td>—</td>
</tr>
<tr>
<td>show</td>
<td>SHOW</td>
<td>Y</td>
<td>Case insensitive</td>
</tr>
<tr>
<td>show</td>
<td>Sh??</td>
<td>Y</td>
<td>Matches any character</td>
</tr>
<tr>
<td>show</td>
<td>Sho??</td>
<td>N</td>
<td>Second &quot;?&quot; intersects with the character that does not exist</td>
</tr>
<tr>
<td>show</td>
<td>S*</td>
<td>Y</td>
<td>&quot;*&quot; matches any character</td>
</tr>
<tr>
<td>show</td>
<td>S*w</td>
<td>Y</td>
<td>&quot;*&quot; matches characters &quot;ho&quot;</td>
</tr>
<tr>
<td>show</td>
<td>S*p</td>
<td>N</td>
<td>Character &quot;p&quot; does not correspond</td>
</tr>
</tbody>
</table>

2. For each matching command, Cisco ISE validates the arguments.

The command set list will include a space-delimited set of arguments for each command.


This command has two arguments.

1. Argument 1: interface[1-4]
The command arguments in the request are taken in the position-significant order they appear in the packet. If all the arguments in the command definition match the arguments in the request, then this command/argument is said to be matched. Note that any extraneous arguments in the request are ignored.

**Note**
Use the standard Unix regular expressions in arguments.

**Process Rules with Multiple Command Sets**

1. If a command set contains a match for the command and its arguments, and the match has Deny Always, ISE designates the command set as Commandset-DenyAlways.

2. If there is no Deny Always for a command match in a command set, ISE checks all the commands in the command set sequentially for the first match.
   1. If the first match has Permit, ISE designates the command set as Commandset-Permit.
   2. If the first match has Deny, ISE designates the command set as Commandset-Deny.

3. After ISE has analyzed all the command sets, it authorizes the command:
   1. If ISE designated any command set as Commandset-DenyAlways, ISE denies the command.
   2. If there is no Commandset-DenyAlways, ISE permits the command if any command set is Commandset-Permit; otherwise, ISE denies the command. The only exception is when the Unmatched check box is checked.

**TACACS+ Profile**

TACACS+ profiles control the initial login session of the device administrator. A session refers to each individual authentication, authorization, or accounting request. A session authorization request to a network device elicits an ISE response. The response includes a token that is interpreted by the network device, which limits the commands that may be executed for the duration of a session. The authorization policy for a device administration access service can contain a single shell profile and multiple command sets. The TACACS+ profile definitions are split into two components:

- Common tasks
- Custom attributes

There are two views in the TACACS+ Profiles page (Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles)—Task Attribute View and Raw View. Common tasks can be entered using the Task Attribute View and custom attributes can be created in the Task Attribute View as well as the Raw View.

The Common Tasks section allows you to select and configure the frequently used attributes for a profile. The attributes that are included here are those defined by the TACACS+ protocol draft specifications. However, the values can be used in the authorization of requests from other services. In the Task Attribute View, the ISE administrator can set the privileges that will be assigned to the device administrator. The common task types are:

- Shell
The Custom Attributes section allows you to configure additional attributes. It provides a list of attributes that are not recognized by the Common Tasks section. Each definition consists of the attribute name, an indication of whether the attribute is mandatory or optional, and the value for the attribute. In the Raw View, you can enter the mandatory attributes using an equal to (=) sign between the attribute name and its value and optional attributes are entered using an asterisk (*) between the attribute name and its value. The attributes entered in the Raw View are reflected in the Custom Attributes section in the Task Attribute View and vice versa. The Raw View is also used to copy paste the attribute list (for example, another product's attribute list) from the clipboard onto ISE. Custom attributes can be defined for nonshell services.

**Common Tasks Settings**

Navigate to Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles > Add to view the common tasks settings page. The Common Task Types are Shell, WLC, Nexus, and Generic.

**Shell**

The following options are available for the ISE administrator to set the device administrator's privileges.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Privilege</td>
<td>Enable the default (initial) privilege level for a device administrator for the shell authorization. Select any one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Select values between 0 through 15.</td>
</tr>
<tr>
<td></td>
<td>• Select the required Identity Store Attribute.</td>
</tr>
<tr>
<td>Maximum Privilege</td>
<td>Enable the maximum privilege level for Enable authentication. You can select values between 0 through 15.</td>
</tr>
<tr>
<td>Access Control List</td>
<td>Select an ASCII String (1-251*) or the required Identity Store Attribute.</td>
</tr>
<tr>
<td>Auto Command</td>
<td>Select an ASCII String (1-248*) or the required Identity Store Attribute.</td>
</tr>
<tr>
<td>No Escape</td>
<td>Select any one of the following options for escape characters:</td>
</tr>
<tr>
<td></td>
<td>• True—Specifies that escape prevention is enabled.</td>
</tr>
<tr>
<td></td>
<td>• False—Specifies that escape prevention is not enabled.</td>
</tr>
<tr>
<td></td>
<td>• Select the required Identity Store Attribute.</td>
</tr>
</tbody>
</table>
Option | Description
---|---
Timeout | Select values between 0 through 9999 or the required Identity Store Attribute.
Idle Time | Select values between 0 through 9999 or the required Identity Store Attribute.

**WLC**

The following options are available for the ISE administrator to control a device administrator's access to the WLC application tabs. The WLC application contains the following tabs: WLAN, Controller, Wireless, Security, Management, and Commands.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Device administrators have full access to all the WLC application tabs.</td>
</tr>
<tr>
<td>Monitor</td>
<td>Device administrators have only read-only access to the WLC application tabs.</td>
</tr>
<tr>
<td>Lobby</td>
<td>Device administrators have only limited configuration privileges.</td>
</tr>
<tr>
<td>Selected</td>
<td>Device administrators have access to the tabs as checked by the ISE administrator from the following check boxes: WLAN, Controller, Wireless, Security, Management, and Commands.</td>
</tr>
</tbody>
</table>

**Nexus**

The following options are available for the ISE administrator to control a device administrator's access to the Cisco Nexus switches.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Attribute As</td>
<td>An ISE administrator can specify the Nexus attributes generated by the common tasks as Optional or Mandatory.</td>
</tr>
</tbody>
</table>
When a Nexus is configured to authenticate using ISE, the device administrator, by default, has read-only access. Device administrators can be assigned to one of these roles. Each role defines the operations that is allowed:

- **None**—No privileges.
- **Operator (Read Only)**—Complete read access to the entire NX-OS device.
- **Administrator (Read/Write)**—Complete read-and-write access to the entire NX-OS device.

### Generic

The ISE administrator uses the option to specify custom attributes that are not available in the common tasks.

## Create TACACS+ Command Sets

To create a policy set using the TACACS+ command sets policy results:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Choose <strong>Work Centers &gt; Device Administration &gt; Policy Elements &gt; Results &gt; TACACS Command Sets</strong>. You can also configure TACACS command sets in the <strong>Work Centers &gt; Device Administration &gt; Device Admin Policy Sets</strong> page.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Click <strong>Add</strong>.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Enter a name and description.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Click <strong>Add</strong> to specify the Grant permission, Command, and Argument.</td>
</tr>
</tbody>
</table>
| **Step 5** | In the **Grant** drop-down, you can choose one of the following:  
  - **Permit**: To allow the specified command, (for example, permit show, permit con* Argument terminal).  
  - **Deny**: To deny the specified command, (for example, deny mtrace).  
  - **Deny Always**: To override a command that has been permitted in any other command set, (for example, clear auditlogs) |

**Note**  
Click the action icon to increase or decrease the column width of the Grant, Command, and Argument fields.
Step 6  Check the Permit any command that is not listed below check box to allow commands and arguments that are not specified as Permit, Deny or Deny Always in the Grant column.

Create TACACS+ Profiles

To create a TACACS+ profile:

Step 1  Choose Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles.
You can also configure TACACS command sets in the Work Centers > Device Administration > Device Admin Policy Sets page.

Step 2  Click Add.

Step 3  In the TACACS Profile section, enter a name and description.

Step 4  In the Task Attribute View tab, check the required Common Tasks. Refer to the Common Tasks Settings, on page 203 page.

Step 5  In the Task Attribute View tab, in the Custom Attributes section, click Add to enter the required attributes.

Create Device Administration Policy Sets

To create a device administration policy set:

Before you begin

- Ensure that the Device Administration in the Work Centers > Device Administration > Overview > Deployment page is enabled for TACACS+ operations.

- Ensure that any User Identity Groups, (for example, System_Admin, Helpdesk) required for the policy are created. (Work Centers > Device Administration > User Identity Groups page). Ensure that the member users (for example, ABC, XYZ) are allocated to their corresponding groups. (Work Centers > Device Administration > Identities > Users page).

- Ensure to configure TACACS settings on devices that need to be administered. (Work Centers > Device Administration > Network Resources > Network Devices > Add > TACACS Authentication Settings check box is enabled and the shared secret for TACACS and devices are identical to facilitate the devices to query ISE.)

- Ensure that the Network Device Group, based on the Device Type and Location, is created. (Work Centers > Device Administration > Network Device Groups page)

Step 1  Choose Work Centers > Device Administration > Device Admin Policy Sets.

Step 2  From the Actions column on any row, click the cog icon and then from the drop-down menu, insert a new policy set by selecting any of the insert or duplicate options, as necessary.
A new row appears in the Policy Sets table.

Step 3  Enter the name and description for the policy set.
Step 4 If required, from the Allowed Protocols/Server Sequence column, click the (+) symbol and select one of the following:
   a) Create a New Allowed Protocol
   b) Create a TACACS Server Sequence

Step 5 From the **Conditions** column, click the (+) symbol.

Step 6 Create the required conditions in the **Conditions Studio Page**. In the Editor section, click the **Click To Add an Attribute** text box, and select the required Dictionary and Attribute (for example, Device-Location Equals Europe). You can drag and drop a Library condition to the **Click To Add An Attribute** text box.

Step 7 Click **Use**.

Step 8 From the View column, click > to access all of the policy set details and to create the authentication and authorization policies as well as policy exceptions.

Step 9 Create the required Authentication policy, (for example, Rule Name: ATN_Internal_Users, Conditions: DEVICE:Location EQUALS Location #All Locations#Europe—The policy matches only devices that are in location Europe).

Step 10 Click **Save**.

Step 11 Create the required Authorization Policy.

Example 1: Rule Name: Sys_Admin_rule, Conditions: if SysAdmin and TACACS User Equals ABC then cmd_Sys_Admin AND Profile_priv_8—The policy matches system administrators with user name ABC and allows the specified commands to be executed and assigns a privilege level of 8.

Example 2: Rule Name: HelpDesk AND TACACS User EQUALS XYZ then cmd_HDesk_show AND cmd_HDesk_ping AND Profile_priv_1—The policy matches system administrators with user name XYZ and allows the specified commands to be executed and assigns a privilege level of 1.

In the above examples:
   • The command sets, cmd_Sys_Admin and cmd_HDesk, are created in the Work Centers > Device Administration > Policy Elements > Results>TACACS Command Sets > Add page.
   • The TACACS profiles, Profile_Priv_1 and Profile_priv_8, are created in the Work Centers > Device Administration > Policy Elements > Results>TACACS Profiles > Add page.

**Note** You can add IPv4 or IPv6 single address for the Device IP address attribute in the conditions used in authentication and authorization policies.

Step 12 Click **Save**.

---

**Monitor Device Administration Activity**

Cisco ISE provides various reports and logs that allow you to view information related to accounting, authentication, authorization, and command accounting of devices configured with TACACS+. You can run these reports either on demand or on a scheduled basis.

Step 1 Choose Work Centers > Device Administration > Reports > ISE Reports. You can also view the reports in the Operations > Reports > ISE Reports page.
Step 2  In the Report Selector, expand Device Administration to view Authentication Summary, TACACS Accounting, TACACS Authentication, TACACS Authorization, TACACS Command Accounting, Top N Authentication by Failure Reason, Top N Authentication by Network Device, Top N Authentication by User reports.

Step 3  Select the report and choose the data with which you want to search using the Filters drop-down list.

Step 4  Select the Time Range during which you want to view the data.

Step 5  Click Run.

---

Configure Global TACACS+ Settings

To configure global TACACS+ settings:

Step 1  Choose Work Centers > Device Administration > Settings.

a) In the Connection Settings tab, you can change the default values for the required fields.

Step 2  In the Password Change Control tab, define the required fields to control whether password update is permitted through TACACS+.

The prompts in the Enable Telnet Change Password section are enabled only when this option is selected. Or else, the prompts in the Disable Telnet Change Password are enabled. The password prompts are fully customizable and can be modified as needed.

In the Password Policy Violation Message field, you can display an appropriate error message for the password set by the internal users if the new password does not match the specified criteria.

Step 3  In the Session Key Assignment tab, select the required fields to link TACACS+ requests into a session.

The session key is used by the Monitoring node to link AAA requests from clients. The default settings are for NAS-Address, Port, Remote-Address, and User fields to be enabled.

Step 4  Click Save.
CHAPTER 10

Manage Network Devices

- Network Devices Definitions in Cisco ISE, on page 209
- Default Network Device Definition in Cisco ISE, on page 210
- Create a Network Device Definition in Cisco ISE, on page 211
- Import Network Devices into Cisco ISE, on page 211
- Export Network Devices from Cisco ISE, on page 212
- Third-Party Network Device Support in Cisco ISE, on page 212
- Network Device Groups, on page 219
- Import Network Device Groups into Cisco ISE, on page 220
- Export Network Device Groups from Cisco ISE, on page 220
- Import Templates in Cisco ISE, on page 221
- IPsec Security to Secure Cisco ISE-NAD Communication, on page 225
- Mobile Device Manager Interoperability with Cisco ISE, on page 236
- Set Up MDM Servers with Cisco ISE, on page 240

Network Devices Definitions in Cisco ISE

A network device such as a switch or a router is an authentication, authorization, and accounting (AAA) client through which AAA service requests are sent to Cisco ISE. You must define network devices for Cisco ISE to interact with the network devices. You can configure network devices for RADIUS or TACACS AAA, Simple Network Management Protocol (SNMP) for the Profiling service to collect Cisco Discovery Protocol and Link Layer Discovery Protocol attributes for profiling endpoints, and Trustsec attributes for Trustsec devices. A network device that is not defined in Cisco ISE cannot receive AAA services from Cisco ISE.

In the network device definition:

- You can select the vendor profile that fits the network device. The profile includes pre-defined configurations for the device, such as settings for URL direct and change of authorization.

- You can configure the RADIUS protocol for RADIUS authentications. When Cisco ISE receives a RADIUS request from a network device, it looks for the corresponding device definition to retrieve the shared secret that is configured. If it finds the device definition, it obtains the shared secret that is configured on the device and matches it against the shared secret in the request to authenticate access. If the shared secrets match, the RADIUS server will process the request further based upon the policy and configuration. If they do not match, a reject response is sent to the network device. A failed authentication report is generated, which provides the failure reason.
• You can configure the TACACS+ protocol for TACACS+ authentications. When Cisco ISE receives a TACACS+ request from a network device, it looks for the corresponding device definition to retrieve the shared secret that is configured. If it finds the device definition, it obtains the shared secret that is configured on the device and matches it against the shared secret in the request to authenticate access. If the shared secrets match, the TACACS+ server will process the request further based upon the policy and configuration. If they do not match, a reject response is sent to the network device. A failed authentication report is generated, which provides the failure reason.

• You can configure the Simple Network Management Protocol (SNMP) in the network device definition for the Profiling service to communicate with the network devices and profile endpoints that are connected to the network devices.

• You must define Trustsec-enabled devices in Cisco ISE to process requests from Trustsec-enabled devices that can be part of the Cisco Trustsec solution. Any switch that supports the Trustsec solution is an Trustsec-enabled device.

Trustsec devices do not use the IP address. Instead, you must define other settings so that Trustsec devices can communicate with Cisco ISE.

Trustsec-enabled devices use the Trustsec attributes to communicate with Cisco ISE. Trustsec-enabled devices, such as the Nexus 7000 series switches, Catalyst 6000 series switches, Catalyst 4000 series switches, and Catalyst 3000 series switches are authenticated using the Trustsec attributes that you define while adding Trustsec devices.

**Default Network Device Definition in Cisco ISE**

Cisco ISE supports the default device definition for RADIUS and TACACS authentications. You can define a default network device that Cisco ISE can use if it does not find a device definition for a particular IP address. This feature enables you to define a default RADIUS or TACACS shared secret and the level of access for newly provisioned devices.

**Note**

We recommend that you add the default device definition only for basic RADIUS and TACACS authentications. For advanced flows, you must add separate device definition for each network device.

Cisco ISE looks for the corresponding device definition to retrieve the shared secret that is configured in the network device definition when it receives a RADIUS or TACACS request from a network device.

Cisco ISE performs the following procedure when a RADIUS or TACACS request is received:

1. Looks for a specific IP address that matches the one in the request.
2. Looks up the ranges to see if the IP address in the request falls within the range that is specified.
3. If both step 1 and 2 fail, it uses the default device definition (if defined) to process the request.

Cisco ISE obtains the shared secret that is configured in the device definition for that device and matches it against the shared secret in the RADIUS or TACACS request to authenticate access. If no device definitions are found, Cisco ISE obtains the shared secret from the default network device definition and processes the RADIUS or TACACS request.
Create a Network Device Definition in Cisco ISE

You can create a network device definition in Cisco ISE and use the default network device definition when there is no network device definition in Cisco ISE.

You can also create the network device definition in the Work Centers > Device Administration > Network Resources > Network Devices page.

Step 1  Choose Administration > Network Resources > Network Devices.
Step 2  Click Add.
Step 3  Complete all mandatory fields.
Step 4  Check the RADIUS Authentication Settings check box to configure the RADIUS protocol for authentication.
Step 5  Check the TACACS Authentication Settings check box to configure the TACACS protocol for authentication.
Step 6  (Optional) Check the SNMP Settings check box to configure the Simple Network Management Protocol for the Profiling service to collect device information.
Step 7  (Optional) Check the Advanced Trustsec Settings check box to configure a Trustsec-enabled device.
Step 8  Click Submit.

Import Network Devices into Cisco ISE

You can import a list of device definitions into a Cisco ISE node using a comma-separated value (CSV) file. You must first update the imported template before you can import network devices into Cisco ISE. You cannot run an import of the same resource type at the same time. For example, you cannot concurrently import network devices from two different import files.

You can download the CSV template from the Admin portal, enter your device definition details in the template, and save it as a CSV file, which you can then import back into Cisco ISE.

While importing devices, you can create new records or update existing records. Cisco ISE displays the summary of the number of devices that are imported and also reports any errors that were found during the import process. When you import devices, you can also define whether you want Cisco ISE to overwrite the existing device definitions with the new definitions or stop the import process when Cisco ISE encounters the first error.

You cannot import network devices that are exported in previous releases of Cisco ISE, as the import template for these releases are different.

**Note**

You can import the network devices with IP ranges in all the octets.

Step 1  Choose Administration > Network Resources > Network Devices.
Step 2  Click Import.
Step 3  Click Browse to choose the CSV file from the system that is running the client browser.
Export Network Devices from Cisco ISE

You can export network devices configured in Cisco ISE in the form of a CSV file that you can use to import these network devices into another Cisco ISE node.

### Note
You can export the network devices with IP ranges in all the octets.

#### Step 1
Choose Administration > Network Resources > Network Devices.

#### Step 2
Click Export.

#### Step 3
To export network devices, you can do one of the following:

- Check the check boxes next to the devices that you want to export, and choose Export > Export Selected.
- Choose Export > Export All to export all the network devices that are defined.

#### Step 4
Save the export.csv file to your local hard disk.

Third-Party Network Device Support in Cisco ISE

Cisco ISE supports third-party network access devices (NADs) through the use of network device profiles. NAD profiles define the capabilities of the third-party device with simplified policy configuration, regardless of the vendor-side implementation. A network device profile contains the following:

- The protocols the network device support, such as RADIUS, TACACS+, and TrustSec. You can import any vendor-specific RADIUS dictionaries that exist for the device into Cisco ISE.
- The attributes and values that the device uses for the various flows such as Wired MAB and 802.1x. This allows Cisco ISE to detect the right flow type for your device according to the attributes it uses.
- The Change of Authorization (CoA) capabilities the device has. While RFC 5176 defines the types of CoA requests, the required attributes in the requests vary depending on the device. Most non-Cisco devices with RFC 5176 support will also support the "Push" and "Disconnect" functions. For devices that do not support the RADIUS CoA type, ISE also supports SNMP CoA. CoA types are described in further detail below.
- The attributes and protocols the device uses for MAB. Network devices from different vendors perform MAB authentication differently.
- The VLAN and ACL permissions used by the device. After the profile is saved, Cisco ISE automatically generates authorization profiles for each configured permission.
• URL redirection is necessary for advanced flows like BYOD, Guest, and Posture. There are two types of URL redirection found on a device: static and dynamic. For static URL redirection, you can copy and paste the ISE portal URL into the configuration. For dynamic URL redirection, ISE uses a RADIUS attribute to tell the network device where to redirect to. In addition, if the device supports neither dynamic nor static URL redirect, ISE provides an Auth VLAN by which it simulates URL redirect. Auth VLAN is based on a DHCP/DNS service running on the ISE box. To create the Auth VLAN, define the DHCP/DNS service settings. For more information, see **DHCP and DNS Services**, on page 967. The URL redirect flow is described in further detail below.

Once you have defined your devices in ISE, configure these device profiles or used the preconfigured device profiles offered by ISE in order to define the capabilities that Cisco ISE uses to enable basic flows, as well as advanced flows such as Profiler, Guest, BYOD, MAB, and Posture.

**URL Redirect Mechanism and Auth VLAN**

When a third-party device is used in the network and the device does not support dynamic or static URL redirect, ISE simulates the URL redirect flow. The URL redirect simulation flow for such devices is operated by running a DHCP/DNS service on the ISE box (For more information, see #unique_343), and the Auth VLAN flow is as follows:

1. A guest endpoint connects to the NAD.
2. The device sends the RADIUS/MAB request to ISE.
3. ISE runs the authentication/authorization policy and stores the user accounting information.
4. ISE sends the RADIUS access/accept message, containing the Auth VLAN ID.
5. The guest endpoint receives network access.
6. The endpoint broadcasts a DHCP request and obtains a client IP address and the ISE sinkhole DNS IP address from the ISE DHCP service.
7. The guest endpoint opens a browser. The browser sends a DNS query and receives the ISE IP address.
8. The endpoint HTTP or HTTPS request is directed to the ISE box.
9. ISE responds with HTTP 301/Moved, providing the guest portal URL. The endpoint browser redirects to the Guest portal page.
10. The guest endpoint user logs in for authentication.
11. Once compliance is validated, ISE responds to the NAD, sending the CoA, authorizing the endpoint and bypassing the sinkhole.
12. Appropriate access is provided to the user based on the CoA, the endpoint receives an IP address from an enterprise DHCP and the user can now use the network.

The Auth VLAN should be separated from the corporate network in order to prevent unauthorized network access by the guest endpoint before the endpoint passes authentication. Configure the Auth VLAN IP helper to point to the ISE machine, or connect one of the ISE network interfaces to the Auth VLAN. For more information about VLAN (DHCP/DNS server) settings, see #unique_343. Multiple VLANs may be connected to one network interface card by configuring a VLAN IP-helper from the NAD configuration. For more information about configuring an IP helper, refer to the administration guide for the device for instructions. In addition, for Guest flows, define a guest portal and select that portal in an Authorization profile that is
bound to MAB authorization, similar to regular Guest flows. For more information about guest portals, see Cisco ISE Guest Services, on page 443.

The following diagram displays the basic network setup when an Auth VLAN is defined (the Auth VLAN is connected directly to the Cisco ISE node):

*Figure 9: Auth VLAN connect to Cisco ISE Node*

The following diagram displays the network with Auth VLAN and an IP helper:

*Figure 10: Auth VLAN with IP Helper*

**CoA Types**

ISE supports both RADIUS and SNMP CoA types. RADIUS or SNMP CoA type support is required in order for the NAD to work in complex flows, while it is not mandatory for basic flows. Define the RADIUS and SNMP settings supported by the device when configuring the NAD from ISE, and indicate the CoA type to be used for a specific flow when configuring the NAD profile. For more information about defining protocols for your NADs, see Network Devices, on page 988. Check with your third party supplier to verify which type your NAD supports prior to creating the device and NAD profile in ISE.
Network Device Profiles

Cisco ISE supports some third-party network access devices (NADs) through the use of network device profiles. These profiles define the capabilities that Cisco ISE uses to enable basic flows, and advanced flows such as Guest, BYOD, MAB, and Posture.

Cisco ISE includes predefined profiles for network devices from several vendors. Cisco ISE 2.1 has been tested with the vendor devices listed in the following table:

Table 8: Vendor Devices Tested With Cisco ISE 2.1

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Vendor</th>
<th>CoA Type</th>
<th>URL Redirect Type</th>
<th>Supported/Validated Use Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless</td>
<td>Aruba 7000, InstantAP</td>
<td>RADIUS</td>
<td>Static URL</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>Motorola RFS 4000</td>
<td>RADIUS</td>
<td>Dynamic URL</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>HP 830</td>
<td>RADIUS</td>
<td>Static URL</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>Ruckus ZD 1200</td>
<td>RADIUS</td>
<td>—</td>
<td>√</td>
</tr>
<tr>
<td>Wired</td>
<td>HP A5500</td>
<td>RADIUS</td>
<td>Auth VLAN provided by ISE</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>HP 3800 and 2920 (ProCurve)</td>
<td>RADIUS</td>
<td>Auth VLAN provided by ISE</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>Alcatel 6850</td>
<td>SNMP</td>
<td>Dynamic URL</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>Brocade ICX 6610</td>
<td>RADIUS</td>
<td>Auth VLAN provided by ISE</td>
<td>√</td>
</tr>
<tr>
<td></td>
<td>Juniper EX3300-24p</td>
<td>RADIUS</td>
<td>Auth VLAN provided by ISE</td>
<td>√</td>
</tr>
</tbody>
</table>
Configure Third-Party Network Device in Cisco ISE

Cisco ISE supports third-party network access devices (NADs) through the use of network device profiles. These profiles define the capabilities that Cisco ISE uses to enable flows such as Guest, BYOD, MAB, and Posture.

Before you begin

Read the definition for Network Device Profiles, on page 215 in the Cisco Identity Services Engine Administration Guide.

Step 1

Ensure your device is configured in ISE. If you are configuring Guest, BYOD, or Posture workflows, ensure Change of Authorization (CoA) is defined and the NAD’s URL redirect mechanism is configured to point at the relevant ISE Portal. For the URL redirect, you can copy the ISE portal URL from the portal’s landing page. For more information about configuring CoA types and URL redirect for the NAD in ISE, see Network Devices, on page 988. In addition, refer to the third party device’s administration guide for instructions.

Step 2

Ensure an appropriate NAD profile for your device is available in ISE. To view existing profiles, choose Administration > Network Resources > Network Device Profiles. If an appropriate profile does not already exist in ISE, create a custom profile. See Create a Network Device Profile, on page 217 for information on how to create custom profiles.

Step 3

Assign a NAD profile to the NAD that you want to configure. Choose Administration > Network Resources > Network Devices. Open the device to which you would like to assign a profile and from Device Profile, select the correct profile from the dropdown list.

Step 4

When you configure your policy rules, the authorization profile should be explicitly set to the NAD profile in step 1, or “Any” if you are just using VLAN or ACL or if you have different devices from different vendors in your network. To set the NAD profile for the authorization profile, choose Policy > Policy Elements > Results > Authorization > Authorization Profiles. Open the relevant authorization profile and from Network Device Profile, select the relevant NAD profile from the dropdown list. When using Auth VLAN for Guest flows, you should also define a guest portal and
Create a Network Device Profile

Before you begin

- For more information about creating a custom profile, read the Network Access Device Profiles with Cisco Identity Services Engine document.

- Most NADs have a vendor-specific RADIUS dictionary that provides a number of vendor-specific attributes in addition to the standard IETF RADIUS attributes. If the network device has a vendor-specific RADIUS dictionary, import it into Cisco ISE. Refer to the third party device’s administration guide for instructions on which RADIUS dictionary is required. From ISE, choose Policy Elements > Dictionaries > System > Radius > RADIUS Vendors. For more information about importing RADIUS dictionaries, see Create RADIUS-Vendor Dictionaries, on page 264.

- For complex flows such as Guest and Posture, the device needs to support RFC 5176, Change of Authorization (CoA).

- For more information about the fields and possible values for creating a network device profile, see Network Device Profiles Settings, on page 1003.

Step 1
Choose Administration > Network Resources > Network Device Profiles.

Step 2
Click Add.

Step 3
Enter a name and description for the network device.

Step 4
Select the vendor of the network device.

Step 5
Check the check boxes for the protocols that the device supports. Check each box if your device supports RADIUS, TACACS+ and/or TrustSec. It is only necessary to check the protocols you want to actually use. If the device supports RADIUS, select the RADIUS dictionary to use with the network device from the dynamic dropdown list in the RADIUS Dictionaries field.

Step 6
From the Templates section, enter relevant details as follows:

a) From Authentication/Authorization configure the device's default settings for flow types, attribute aliasing, and host lookup: From Flow Type Conditions, enter the attributes and values that your device uses for the various flows such as Wired MAB, or 802.1x. This enables ISE to detect the correct flow type for your device according to the attributes it uses. There is no IETF standard for MAB and different vendors use different values for Service-Type. Refer to the device's user guide or use a sniffer trace of a MAB authentication to determine the correct settings. From Attribute Aliasing, map device specific attribute names to common names to simplify policy rules. Currently, only SSID is defined. If your device has the concept of wireless SSID and then to set this to the attribute it uses. ISE maps this to an attribute called SSID in the Normalised Radius dictionary. This simplifies policy rule configuration as you can refer to SSID in one rule and it will work for multiple devices even if the underlying attributes are different. From Host Lookup, enable the Process Host Lookup option and select the relevant MAB protocols and attributes for your device, based on the third-party instructions.

b) From Permissions configure the network device's default settings for VLAN and ACL. These are automatically mapped based on the authorization profiles you created in ISE.

c) From Change of Authorization (CoA) configure the device's CoA capabilities.
d) Expand the Redirect section to configure the device's URL redirect capabilities. URL redirection is necessary for Guest, BYOD, and Posture.

Step 7  Click Submit.

### Export Network Device Profiles from Cisco ISE

Export single or multiple network device profiles configured in Cisco ISE in the form of an XML file in order to edit the XML file and then import the file as new network profiles.

**Before you begin**

Read the Network Access Device Profiles with Cisco Identity Services Engine document.

**Step 1**  Choose Administration > Network Resources > Network Device Profiles.
**Step 2**  Click Export.
**Step 3**  Check the check boxes next to the devices that you want to export, and choose Export > Export Selected
**Step 4**  The DeviceProfiles.xml file downloads to your local hard disk.

### Import Network Device Profiles into Cisco ISE

You can import a single or multiple network device profiles into ISE using a single XML file with the Cisco ISE XML structure. You cannot concurrently import network device profiles from multiple import files.

Typically, you would first export an existing profile from the Admin portal to use as a template. Enter your device profile details as necessary in the file and save it as an XML file, and then import the edited file back in to Cisco ISE. In order to work with multiple profiles, you can export multiple profiles structured together as a single XML file, edit the file and then import them together, creating multiple files in ISE.

While importing device profiles, you can only create new records. You cannot overwrite an existing profile. In order to edit an existing profile and then overwrite it, export the existing profile, delete the profile from ISE and then import that profile once you have edited it accordingly.

**Before you begin**

Read the Network Access Device Profiles with Cisco Identity Services Engine document.

**Step 1**  Choose Administration > Network Resources > Network Device Profiles.
**Step 2**  Click Import.
**Step 3**  Click Browse to choose the XML file from the system that is running the client browser.
**Step 4**  Click Import.
Network Device Groups

Cisco ISE allows you to create hierarchical Network Device Groups (NDGs). NDGs can be used to logically group network devices based on various criteria, such as geographic location, device type, or the relative place in the network (Access Layer, Data Center, and so on). For example, to organize your network devices based on geographic location, you can group them by continent, region, or country:

- Africa -> Southern -> Namibia
- Africa -> Southern -> South Africa
- Africa -> Southern -> Botswana

You can also group the network devices based on the device type:

- Africa -> Southern -> Botswana -> Firewalls
- Africa -> Southern -> Botswana -> Routers
- Africa -> Southern -> Botswana -> Switches

Network devices can be assigned to one or more hierarchical NDGs. Thus, when Cisco ISE processes the ordered list of configured NDGs to determine the appropriate group to assign to a particular device, it may find that the same device profile applies to multiple Device Groups, and will apply the first Device Group matched.

There is no limit on the maximum number of NDGs that can be created. You can create up to 6 levels of hierarchy (including the parent group) for the NDGs.

You can view the device group hierarchy in Tree view or Flat Table view. In the Tree view, the root node appears at the top of the tree followed by the child groups in hierarchical order. Click Expand All to view all the device groups under each root group. Click Collapse All to list only the root groups.

In the Flat Table view, you can view the hierarchy of each device group in the Group Hierarchy column.

You can also view the number of network devices that are assigned to each child group. Click the number link to launch the Network Devices window, which lists all the network devices that are assigned to that device group. You can add additional devices to a device group or move the existing devices to another device group.

While adding a device group, you can specify whether the new group must be added as a root group or select an already existing group as the parent group.

Note

You cannot delete a device group if any devices are assigned to that device group. Before deleting a device group you must move all the existing devices to another device group.

Root Network Device Groups

Cisco ISE includes two predefined root NDGs: All Device Types and All Locations. You cannot edit, duplicate, or delete these predefined NDGs, but you can add new device groups under them.

You can create a root Network Device Group (NDG), and then create child NDGs under the root group in the Network Device Groups page.
Network Device Attributes Used By Cisco ISE in Policy Evaluation

When you create a new network device group, a new network device attribute is added to the Device dictionary defined in the system, which you can use in policy definitions. Cisco ISE allows you to configure authentication and authorization policies based on Device dictionary attributes, such as device type, location, model name, and software version that is running on the network device.

Import Network Device Groups in to Cisco ISE

You can import network device groups into a Cisco ISE node using a comma-separated value (CSV) file. You cannot run import of the same resource type at the same time. For example, you cannot concurrently import network device groups from two different import files.

You can download the CSV template from the Admin portal, enter your device group details in the template, and save the template as a CSV file, which you can then import back into Cisco ISE.

While importing device groups, you can create new records or update existing records. When you import device groups, you can also define whether you want Cisco ISE to overwrite the existing device groups with the new groups or stop the import process when Cisco ISE encounters the first error.

Step 1  Choose Administration > Network Resources > Network Device Groups > Groups.
Step 2  Click Import.
Step 3  Click Browse to choose the CSV file from the system that is running the client browser.
Step 4  Check the Overwrite Existing Data with New Data check box.
Step 5  Check the Stop Import on First Error check box.
Step 6  Click Import or click the Network Device Groups List link to return to the Network Device Groups list page.

Export Network Device Groups from Cisco ISE

You can export network device groups configured in Cisco ISE in the form of a CSV file that you can use to import these network device groups into another Cisco ISE node.

Step 1  Choose Administration > Network Resources > Network Device Groups > Groups.
Step 2  To export the network device groups, you can do one of the following:
  • Check the check boxes next to the device groups that you want to export, and choose mExport > Export Selected.
  • Choose Export > Export All to export all the network device groups that are defined.
Step 3  Save the export.csv file to your local hard disk.
Import Templates in Cisco ISE

Cisco ISE allows you to import a large number of network devices and network device groups using comma-separated value (CSV) files. The template contains a header row that defines the format of the fields. The header row should not be edited, and should be used as is.

By default, you can use the Generate a Template link to download a CSV file in the Microsoft Office Excel application and save the file format locally on your system. When you click the Generate a Template link, the Cisco ISE server displays the Opening template.csv dialog. This dialog allows you to open the template.csv file and save the template.csv file locally on your system with an appropriate name for network devices and network device groups. If you choose to open the template.csv file from the dialog, the file opens in the Microsoft Office Excel application by default.

Network Devices Import Template Format

The following table lists the fields in the template header and provides a description of the fields in the Network Device CSV file.

Table 9: CSV Template Fields and Description for Network Devices

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:String(32):</td>
<td>(Required) This field is the network device name. It is an alphanumeric string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>Description:String(256)</td>
<td>This field is an optional description for the network device. A string, with a maximum of 256 characters in length.</td>
</tr>
<tr>
<td>IP Address:Subnets(a.b.c.d/m</td>
<td>...) (Required) This field is the IP address and subnet mask of the network device. (It can take on more than one value separated by a pipe “</td>
</tr>
<tr>
<td>Model Name:String(32):</td>
<td>(Required) This field is the network device model name. It is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>Software Version:String(32):</td>
<td>(Required) This field is the network device software version. It is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>Network Device Groups:String(100):</td>
<td>(Required) This field should be an existing network device group. It can be a subgroup, but must include both the parent and subgroup separated by a space. It is a string, with a maximum of 100 characters, for example, Location#All Location#US</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Authentication:Protocol: String(6)</td>
<td>This is an optional field. It is the protocol that you want to use for authentication. The only valid value is RADIUS (not case sensitive).</td>
</tr>
<tr>
<td>Authentication:Shared Secret: String(128)</td>
<td>(Required, if you enter a value for the Authentication Protocol field) This field is a string, with a maximum of 128 characters in length.</td>
</tr>
<tr>
<td>EnableKeyWrap: Boolean(true</td>
<td>false)</td>
</tr>
<tr>
<td>EncryptionKey: String(ascii:16</td>
<td>hexa:32)</td>
</tr>
<tr>
<td>AuthenticationKey: String(ascii:20</td>
<td>hexa:40)</td>
</tr>
<tr>
<td>InputFormat: String(32)</td>
<td>Indicates encryption and authentication keys input format. Valid value is ASCII or Hexadecimal.</td>
</tr>
<tr>
<td>SNMP:Version: Enumeration ([2c</td>
<td>3])</td>
</tr>
<tr>
<td>SNMP:RO Community: String(32)</td>
<td>(Required, if you enter a value for the SNMP Version field) SNMP Read Only community. It is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>SNMP:RW Community: String(32)</td>
<td>(Required, if you enter a value for the SNMP Version field) SNMP Read Write community. It is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>SNMP:Username: String(32)</td>
<td>This is an optional field. It is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>SNMP:Security Level: Enumeration(Auth</td>
<td>No Auth</td>
</tr>
<tr>
<td>SNMP:Authentication Protocol: Enumeration(MD5</td>
<td>SHA)</td>
</tr>
<tr>
<td>SNMP:Authentication Password: String(32)</td>
<td>(Required if you have entered Auth for the SNMP security level) It is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SNMP:Privacy Protocol:Enumeration(DES</td>
<td>AES128</td>
</tr>
<tr>
<td>SNMP:Privacy Password:String(32)</td>
<td>(Required if you have entered Priv for the SNMP security level) It is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>SNMP:Polling Interval:Integer:600-86400 seconds</td>
<td>This is an optional field to set the SNMP polling interval. Valid value is an integer between 600 and 86400.</td>
</tr>
<tr>
<td>SNMP:Is Link Trap Query:Boolean(true</td>
<td>false)</td>
</tr>
<tr>
<td>SNMP:Is MAC Trap Query:Boolean(true</td>
<td>false)</td>
</tr>
<tr>
<td>SNMP:Originating Policy Services Node:String(32)</td>
<td>This is an optional field. Indicates which ISE server to be used to poll for SNMP data. By default, it is automatic, but you can overwrite the setting by assigning different values.</td>
</tr>
<tr>
<td>Trustsec:Device Id:String(32)</td>
<td>This is an optional field. It is the Trustsec device ID, and is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>Trustsec:Device Password:String(256)</td>
<td>(Required if you have entered Trustsec device ID) This is the Trustsec device password and is a string, with a maximum of 256 characters in length.</td>
</tr>
<tr>
<td>Trustsec:Environment Data Download Interval:Integer:1-2147040000 seconds</td>
<td>This is an optional field. It is the Trustsec environment data download interval. Valid value is an integer between 1 and 2147040000.</td>
</tr>
<tr>
<td>Trustsec:Peer Authorization Policy Download Interval:Integer:1-2147040000 seconds</td>
<td>This is an optional field. It is the Trustsec peer authorization policy download interval. Valid value is an integer between 1 and 2147040000.</td>
</tr>
<tr>
<td>Trustsec:Reauthentication Interval:Integer:1-2147040000 seconds</td>
<td>This is an optional field. It is the Trustsec reauthentication interval. Valid value is an integer between 1 and 2147040000.</td>
</tr>
<tr>
<td>Trustsec:SGACL List Download Interval:Integer:1-2147040000 seconds</td>
<td>This is an optional field. It is the Trustsec SGACL list download interval. Valid value is an integer between 1 and 2147040000.</td>
</tr>
<tr>
<td>Trustsec:Is Other Trustsec Devices Trusted:Boolean(true</td>
<td>false)</td>
</tr>
</tbody>
</table>
### Network Device Groups Import Template Format

The following table lists the fields in the template header and provides a description of the fields in the Network Device Group CSV file.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trustsec:Notify this device about Trustsec configuration changes:String(ENABLE_ALL</td>
<td>DISABLE_ALL)</td>
</tr>
<tr>
<td>Trustsec:Include this device when deploying Security Group Tag Mapping Updates:Boolean(true</td>
<td>false)</td>
</tr>
<tr>
<td>Deployment:Execution Mode Username:String(32)</td>
<td>This is an optional field. It is the username that has privileges to edit the device configuration. It is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>Deployment:Execution Mode Password:String(32)</td>
<td>This is an optional field. It is the device password and is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>Deployment:Enable Mode Password:String(32)</td>
<td>This is an optional field. It is the enable password of the device that would allow you to edit its configuration and is a string, with a maximum of 32 characters in length.</td>
</tr>
<tr>
<td>Trustsec:PAC issue date:Date</td>
<td>This is the field that displays the issuing date of the last Trustsec PAC that has been generated by Cisco ISE for the Trustsec device.</td>
</tr>
<tr>
<td>Trustsec:PAC expiration date:Date</td>
<td>This is the field that displays the expiration date of the last Trustsec PAC that has been generated by Cisco ISE for the Trustsec device.</td>
</tr>
<tr>
<td>Trustsec:PAC issued by:String</td>
<td>This is a field that displays the name of the issuer (a Trustsec administrator) of the last Trustsec PAC that has been generated by Cisco ISE for the Trustsec device. It is a string.</td>
</tr>
</tbody>
</table>
**Table 10: CSV Template Fields and Description for Network Device Groups**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:String(100):</td>
<td>(Required) This field is the network device group name. It is a string with a maximum of 100 characters in length. The full name of an NDG can have a maximum of 100 characters in length. For example, if you are creating a subgroup India under the parent groups Global &gt; Asia, then the full name of the NDG that you are creating would be Global#Asia#India and this full name cannot exceed 100 characters in length. If the full name of the NDG exceeds 100 characters in length, the NDG creation fails.</td>
</tr>
<tr>
<td>Description:String(1024)</td>
<td>This is an optional network device group description. It is a string, with a maximum of 1024 characters in length.</td>
</tr>
<tr>
<td>Type:String(64):</td>
<td>(Required) This field is the network device group type. It is a string, with a maximum of 64 characters in length.</td>
</tr>
<tr>
<td>Is Root:Boolean(true</td>
<td>false):</td>
</tr>
</tbody>
</table>

---

**IPsec Security to Secure Cisco ISE-NAD Communication**

Internet Protocol security (IPsec) is a set of protocols that provides security to Internet Protocol. The AAA protocols, RADIUS and TACACS+, use the MD5 hashing algorithm. For greater security, Cisco ISE offers the IPsec feature. IPsec provides secure communication by authenticating the sender, discovering any changes in data during transmission, and encrypting the data that is sent.

Cisco ISE supports IPsec in Tunnel and Transport modes. When you enable IPsec on a Cisco ISE interface and configure the peers, an IPsec tunnel is created between Cisco ISE and the NAD to secure the communication.

You can define a pre-shared key or use X.509 certificates for IPsec authentication. IPsec can be enabled on Gigabit Ethernet 1 through Gigabit Ethernet 5 interfaces. You can configure IPsec on only one Cisco ISE interface per PSN.

**Note**

Gigabit Ethernet 0 and Bond 0 (when Gigabit Ethernet 0 and Gigabit Ethernet 1 interfaces are bonded) are management interfaces in the Cisco ISE CLI; IPsec is not supported on Gigabit Ethernet 0 and Bond 0.

Required components include:

- Cisco ISE, Release 2.2
• Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2 (Cisco 5921 Embedded Services Router (ESR))—The ESR 5921 configuration, by default, supports IPsec in Tunnel and Transport modes. Diffie-Hellman Group 14 and Group 16 are supported.

Note The C5921 ESR software is bundled with Cisco ISE, Release 2.2. You need an ESR license to enable it. See Cisco 5921 Embedded Services Router Integration Guide for ESR licensing information.

Configure RADIUS IPsec on Cisco ISE

To configure RADIUS IPsec on Cisco ISE, you must:

Step 1 Configure IP address on the interface from the Cisco ISE CLI.
Gigabit Ethernet 1 through Gigabit Ethernet 5 interfaces (Bond 1 and Bond 2) support IPsec. However, IPsec can be configured on only one interface in a Cisco ISE node.

Step 2 Add a directly-connected network device to the IPsec network device group.

Note RADIUS IPsec requires the static route gateway to be directly connected through an interface of the device.

a) Choose Administration > Network Resources > Network Devices.
b) In the Network Devices page, click Add.
c) Enter the name and IP address and subnet of the network device that you want to add.
d) From the IPSEC drop-down list, choose Yes.
e) Check the RADIUS Authentication Settings checkbox.
f) In the Shared Secret field, enter the shared secret key that you have configured on the network device.
g) Click Submit.

Step 3 (Optional; required only for Smart Licensing) Add a separate management interface to interact with the Cisco Smart Software Manager (CSSM). You can also use Smart Software Manager satellite for ESR. To do this, from the Cisco ISE CLI, run the following command to select the corresponding management interface (Gigabit Ethernet 1-5 (or Bond 1 or 2)):

```
ise/admin# license esr smart {interface}
```
This interface must be able to reach Cisco.com to access the Cisco online licensing server.

Step 4 Add a network device to a directly-connected gateway from the Cisco ISE CLI.

```
ip route [destination network] [network mask] gateway [next-hop address]
```

Step 5 Activate Cisco ISE nodes for IPsec.
a) Choose Administration > System > Settings > Protocols > IPsec.
   All the Cisco ISE nodes in the deployment are listed in this page.
b) Check the check box next to the Cisco ISE node on which you want to activate IPsec, and then click the Enable radio button.
c) Select the interface that you want to use for IPsec communication.
d) Choose an authentication type for the selected ISE node from the following options:

- **Pre-shared Key**—If you choose this option, you must enter the pre-shared key and configure the same key on the network device. Use alphanumeric characters for the pre-shared key. Special characters are not supported. For instructions on how to configure the pre-shared key on the network device, see the network device documentation. For an example of the pre-shared key configuration output, see Example: Output of PreShared Key Configuration on Cisco Catalyst 3850, on page 235.

- **X.509 Certificates**—If you choose this option, from the Cisco ISE CLI, go to the ESR shell and configure and install X.509 Certificates for ESR 5921. Then, configure the network device for IPsec. For instructions, see Configure and Install X.509 Certificates on ESR-5921, on page 229.

e) Click **Save**.

**Note** You cannot modify IPsec configuration directly. If you want to modify the tunnel or authentication when IPsec is enabled, disable the current IPsec tunnel, modify the IPsec configuration and then re-enable the IPsec tunnel with a different configuration.

**Note** If enabled, IPsec removes the IP address from the Cisco ISE interface and shuts down the interface. When the user logs in from Cisco ISE CLI, the interface is displayed with no IP address and in shutdown state. This IP address will be configured on the ESR-5921 interface.

### Step 6

Type `esr` to enter into the ESR shell.

```
ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921_I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.
Press RETURN to get started, CTRL-C to exit
ise-esr5921>
```

**Note** For FIPS compliance, you must configure a secret password of at least 8 characters in length. Enter the **Enable secret level 1** command to specify the password:

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

**Note** If you configure customized RADIUS ports from the GUI (other than 1645, 1646, 1812, and 1813), you must enter the following CLI command in the ESR shell to accept the RADIUS port(s) that are configured:

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

### Step 7

(Optional; required only if you have not enabled Smart Licensing in Step 3) Add a Classic license or an Evaluation license (that is valid for 90 days) to Cisco ISE appliances.

- Run the following command from the Cisco ISE CLI to download the license file:

  ```
  ise/admin# license esr classic import esr.lic repository esrrepo
  ```
For more information on Classic licensing, see the section: Licensing the Software with Classic Licensing in Cisco 5921 Embedded Services Router Integration Guide.

Step 8 Verify IPsec tunnel and RADIUS authentication over IPsec tunnel.
   a) Add a user in Cisco ISE and assign to the user group (Administration > Identity Management > Identities > Users).
   b) Verify if the IPsec tunnel is established between Cisco ISE and the NAD. To do this:
      1. Use the ping command to test if the connection between Cisco ISE and the NAD is established.
      2. Run the following command from the ESR shell or the NAD CLI to verify if the connection is in Active state:
         ```
         show crypto isakmp sa
         ```
         ```
         ise-esr5921#show crypto isakmp sa
         IPv4 Crypto ISAKMP SA
         dst src state conn-id status
         192.168.30.1 192.168.30.3 QM_IDLE 1001 ACTIVE
         ```
      3. Run the following command from the ESR shell or the NAD CLI to verify if the tunnel is established: show crypto ipsec sa
         ```
         ise-esr5921#show crypto ipsec sa
         ```
         ```
         interface: Ethernet0/0
         Crypto map tag: radius, local addr 192.168.30.1
         protected vrf: (none)
         local ident (addr/mask/prot/port): (192.168.30.1/255.255.255.255/0/0)
         remote ident (addr/mask/prot/port): (192.168.30.2/255.255.255.255/0/0)
         current peer 192.168.30.2 port 500
         PERMIT, flags={} #pkts encaps: 52, #pkts encrypt: 52, #pkts digest: 52
         #pkts decaps: 57, #pkts decrypt: 57, #pkts verify: 57
         #pkts compressed: 0, #pkts decompressed: 0
         #pkts not compressed: 0, #pkts compr. failed: 0
         #pkts not decompressed: 0, #pkts decompress failed: 0
         #send errors 0, #recv errors 0
         local crypto endpt.: 192.168.30.1, remote crypto endpt.: 192.168.30.2
         plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/0
         current outbound spi: 0x393783B6(959939510)
         PFS (Y/N): N, DH group: none
         inbound esp sas:
         spi: 0x8EA0F6EE(2392913646)
         transform: esp-aes esp-sha256-hmac ,
         in use settings ={Tunnel, }
         conn id: 99, flow_id: SW:99, sibling_flags 80000040, crypto map: radius
         sa timing: remaining key lifetime (k/sec): (4237963/2229)
         IV size: 16 bytes
         replay detection support: Y
         Status: ACTIVE(ACTIVE)
         inbound ah sas:
         inbound pcp sas:
         outbound esp sas:
         spi: 0x393783B6(959939510)
         transform: esp-aes esp-sha256-hmac ,
         in use settings ={Tunnel, }
         conn id: 100, flow_id: SW:100, sibling_flags 80000040, crypto map: radius
sa timing: remaining key lifetime (k/sec): (4237970/2229)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:

c) Verify the RADIUS authentication using one of the following methods:
   • Log in to the network device using the credentials of the user that you created in Step 8 (a). The RADIUS authentication request is sent to the Cisco ISE node. View the details in the Live Authentications page.
   • Connect the end host with the network device and configure 802.1X authentication. Log in to the end host using the credentials of the user that you created in Step 8 (a). The RADIUS authentication request is sent to the Cisco ISE node. View the details in the Live Authentications page.

---

**Configure and Install X.509 Certificates on ESR-5921**

To configure and install X.509 Certificates on ESR-5921:

---

**Step 1**

Type `esr` to enter into the ESR shell.

```
ise/admin# esr
% Entering ESR 5921 shell
% Cisco IOS Software, C5921 Software (C5921-I86-UNIVERSALK9-M), Version 15.5(2)T2, RELEASE SOFTWARE (fc3)
% Technical Support: http://www.cisco.com/techsupport
% Copyright (c) 1986-2015 Cisco Systems, Inc.

Press RETURN to get started, CTRL-C to exit
```

```
ise-esr5921>
ise-esr5921>
```

**Note** For FIPS compliance, you must configure a secret password of at least 8 characters in length. Enter the **Enable secret level 1** command to specify the password:

```
ise-esr5921(config)#enable secret level 1 ?
0 Specifies an UNENCRYPTED password will follow
5 Specifies a MD5 HASHED secret will follow
8 Specifies a PBKDF2 HASHED secret will follow
9 Specifies a SCRYPT HASHED secret will follow
LINE The UNENCRYPTED (cleartext) 'enable' secret
```

**Note** If you configure customized RADIUS ports from the GUI (other than 1645, 1646, 1812, and 1813), you must enter the following CLI command in the ESR shell to accept the RADIUS port(s) that are configured:

```
ip nat inside source static udp 10.1.1.2 [port_number] interface Ethernet0/0 [port_number]
```

**Step 2** Generate an RSA key pair using the following command:

**Example:**

```
crypto key generate rsa label rsa2048 exportable modulus 2048
```
Step 3  Create a trust point using the following command:

Example:
```
crypto pki trustpoint trustpoint-name
enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=networkdevicename.cisco.com
revocation-check none
rsakeypair rsa2048
```

Step 4  Generate a CSR using the following command:

Example:
```
crypto pki enroll rsaca-mytrustpoint
Display Certificate Request to terminal? [yes/no]: yes
```

Step 5  Copy the output of the CSR to a text file, submit it to an external CA for signing, and obtain the signed certificate and the CA certificate.

Step 6  Import the CA using the following command:

Example:
```
crypto pki authenticate rsaca-mytrustpoint
Copy and paste the contents of the CA certificate, including the “—BEGIN—” and “—End—” lines.
```

Step 7  Import the signed certificate using the following command:

Example:
```
crypto pki import rsaca-mytrustpoint
Copy and paste the contents of the signed certificate, including the “—BEGIN—” and “—End—” lines.
```

Following is an example output when you configure and install X.509 Certificates on Cisco 5921 ESR:
```
is-esr5921#show running-config
!
hostname ise-esr5921
!
boot-start-marker
boot host unix:default-config
boot-end-marker
!
no aaa new-model
bsd-client server url https://cloudsso.cisco.com/as/token.oauth2
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
call-home
!
If contact email address in call-home is configured as sch-smart-licensing@cisco.com
!
If email address configured in Cisco Smart License Portal will be used as contact email address
to send SCH notifications.
contact-email-addr sch-smart-licensing@cisco.com
profile "CiscoTAC-1"
active
destination transport-method http
no destination transport-method email
```
! ip cef
no ipv6 cef
!
! multilink bundle-name authenticated
!
crypto pki trustpoint SLA-TrustPoint
enrollment pkcs12
revocation-check crl
!
crypto pki trustpoint rsaca-mytrustpoint
enrollment terminal
serial-number none
fqdn none
ip-address none
subject-name cn=ise-5921.cisco.com
revocation-check none
rsakeypair rsa2048
!
crypto pki certificate chain SLA-TrustPoint
certificate ca 01
30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
36F2046F 53656E73 696E6772 526F6F74 20434130 1E170D31 33303533 30313934
3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 04031317
43697363 6F312030 1E060355 04031317 43697363 6F2046CF 63656E73 696E6772
526F6F74 20434130 82012230 0D06092A 846866F7 0D010101 05000382 010F0030
82010A02 82010D02 06B6C09C 131E0F7C 145EA72C 2CD686E6 17222E72 1F1EF664
CBB4C798 212AA147 65550BD7 9471380D 8711441E 12AF071A 9D3E6388 8A3E8E52
13C94D78 462EF239 6C957185 B98C0A59 5BB58CB6 0CFEBEA3 700A8BF7 D8F25E6E
4AA4B08D DB6FD1C9 681F8C6F 6FA86957 A2611D7E 104FDC5F EA2956AC
739A3EB5 2B5436AD C874A2C5 DAB55E3B 69A94A35 5B8E9F3E C0BD23CF 5B8D7F88
68896941 20320HE7 948E71D7 AE3BC8C8 F16864C7 4BC8E00F 539BA42B 42C668BB
C747F906 44B2C6E2 E2AF505D C7B024A4 681D195E E8250FC4 5D505FB8 8F27D191
C55F0D76 61944C3D 39923276 A8B03B8D 46D7D609 7CB4F98B 0DF54368 95135844
DFFC7C6F 04DF7DF1 20300D01 01A43230 40300E06 0355100F 0101FF04 04030201
60300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0041604 1449D8C5
4B3D1E83 1B3E6A17 606AF333 3D3B4C73 E8300006 092A8648 86F7D001 010B0500
03820101 015007F24 D392A6A6 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
604DEDCD FF4FDEB2 77CF4C6E CD63F6DB DD446EB1 3A5673AB 903D3B11 6C9E3DBB
D99987BF E40CB9DE 1AECAC02 2189BB5C 8F8A5868 CD98B546 57581468 8D8C66A8
463AD34F 4D565700 6A0F00FD CF850015 3C04F77C 21EB87AC 1B19C2D5 5A5A232C
7CA7B7E6 C1AF74F6 152E9B91 B1FC98B8 E973DE7F 5BEDEB86 C71E3B49 1765308B
5F8B50A6 B92AF7EF 49E88ACE 07B85737 F3A58BEE 1A4A229 C37C1869 39FD8678
82DCCD16 6DB6CECA EEEC7CF9 8428878B 35202C0D 60E4616A B623CDDB 230E3AFB
418616A9 409E049F 4D10AB75 27E86F73 9323E5B5 8862F3DF 0275156F 719BB2F0
D697DF7F 28
quit

crypto pki certificate chain rsaca-mytrustpoint
certificate ca 39
30820386 3082026E A0030201 02020139 300D0609 2A864886 F70D0101 0B050030
61310BD3 0B060355 04061302 55350030 30090603 5504080C 024E4303 0C300A06
03550407 0C035254 50310E30 0C060355 0400A0C5 43493543 4F310CC0 0A006355
0400B0C3 53544F31 19301706 03505403 0C017273 6163162E 65723638 616F2E63
6FFD301E 170D3136 30350031 32130337 34335167 0D313730 39303132 31303734
353A301D 311B3019 06035504 0313269 73652035 3932312E 63967363 6F2E630F
6D308B21 22300D06 092A8648 86F7D001 01010500 0382010F 00308201 00A28201
0100E8E7 CABFBFA1 7E0405AB ACAAAE237 C876B109 2C9FF8AB E8E93536 BF1E83F3
73E60BE7 F430B5AF EBF8B0C5 969282B8 A6783BB4 64E333E4 29C8744E 67E83167
194AF1BU 7E048AE4 B99FD6EB F9C4F2D0 16936E66 CAA498BB 665B6KD 2FBEC1D2
8E8181B9 65AEAE12 1B2E4E4 1F32A197 101CB176 A2CB3174 361B3431A 2CB79BFE
22C0C33F 2792D714 C4122373 081BAE49 69593DC3 A799D526 D81F9706 A71D1A4E
7E765E56 7A2C48A4 C66E835C 337BA1D3 9CA56AC2 C8E0059F 660CE39C 9251310D
F9A21FFB 3C3C507A 20B924F7 E0125D60 6552321C 35736079 42449401 15E6826A
Cisco Identity Services Engine Administrator Guide, Release 2.2
Certificate ca 008DD3A81106B14664

Certificate ca 008DD3A81106B14664

Certificate ca 008DD3A81106B14664

Certificate ca 008DD3A81106B14664

Certificate ca 008DD3A81106B14664

Certificate ca 008DD3A81106B14664

Certificate ca 008DD3A81106B14664

Certificate ca 008DD3A81106B14664

Certificate ca 008DD3A81106B14664

Certificate ca 008DD3A81106B14664

Certificate ca 008DD3A81106B14664
crypto isakmp policy 20
encr aes
hash sha256
group 14
crypto isakmp profile MVPN-profile
    description LAN-to-LAN for spoke router(s) connection
    keying MVPN-spokes
    match identity address 0.0.0.0
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel
crypto ipsec transform-set radius-2 esp-aes esp-sha256-hmac
mode transport
!
crypto dynamic-map MVPN-dynmap 10
set transform-set radius radius-2
!
crypto map radius 10 ipsec-isakmp dynamic MVPN-dynmap
!
interface Ethernet0/0
description e0/0->connection to external NAD
ip address 192.168.20.1 255.255.255.0
ip nat outside
ip virtual-reassembly in
no ip route-cache
crypto map radius
!
interface Ethernet0/1
description e0/1->tap0 internal connection to ISE
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
no ip route-cache
!
interface Ethernet0/2
no ip address
shutdown
!
interface Ethernet0/3
no ip address
shutdown
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
!
access-list 1 permit 10.1.1.0 0.0.0.3
!
control-plane
!
line con 0
logging synchronous
line aux 0
line vty 0 4
login
transport input none
!
end
Following is an example output when you configure and install X.509 Certificates on Cisco Catalyst 3850:

```bash
cat3850#show running-config
enable password lab
!
username lab password 0 lab
aaa new-model
!

aaa group server radius ise
server name ise-vm
deadtime 60
!

aaa authentication login default group radius local
aaa authentication enable default group radius enable
!
crypto isakmp policy 10
encr aes
hash sha256
authentication rsa-sig
group 16
!
crypto ipsec security-association lifetime seconds 86400
!
crypto ipsec transform-set radius esp-aes esp-sha256-hmac
mode tunnel
!
crypto ipsec profile radius-profile
!
crypto map radius 10 ipsec-isakmp
set peer 192.168.20.1
set transform-set radius
match address 100
!
interface GigabitEthernet1/0/1
no switchport
ip address 192.168.20.2 255.255.255.0

crypto map radius
!
access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
!
snmp-server community public RO
snmp-server community private RW
!
radius server rad-ise
address ipv4 192.168.20.1 auth-port 1645 acct-port 1646
```
Example: Output of PreShared Key Configuration on Cisco Catalyst 3850

Following is an example of the output when you configure the pre-shared key on Cisco Catalyst 3850:

cat3850#show running-config

enable password lab
!
username lab password 0 lab
aaa new-model
!
aaa group server radius ise
server name ise-vm
deadtime 60
!
aaa authentication login default group radius local

aaa authentication enable default group radius enable
!
crypto isakmp policy 10

  encr aes
  hash sha256
  authentication pre-share
  group 16
  crypto isakmp key 123456789 address 0.0.0.0
  !
  crypto ipsec security-association lifetime seconds 86400
  !
  crypto ipsec transform-set radius esp-aes esp-sha256-hmac
  mode tunnel
  !
  crypto ipsec profile radius-profile
  !
  crypto map radius 10 ipsec-isakmp
  set peer 192.168.20.1
  set transform-set radius
  match address 100
  !
  interface GigabitEthernet1/0/1
  no switchport
  ip address 192.168.20.2 255.255.255.0

  crypto map radius
  !
  access-list 100 permit ip host 192.168.20.2 host 192.168.20.1
  !
  snmp-server community public RO
  snmp-server community private RW
  !
  radius server rad-ise
  address ipv4 192.168.20.1 auth-port 1645 acct-port 1646

  key secret
Mobile Device Manager Interoperability with Cisco ISE

Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices deployed across mobile operators, service providers, and enterprises. MDM servers act as a policy server that controls the use of some applications on a mobile device (for example, an e-mail application) in the deployed environment. However, the network is the only entity that can provide granular access to endpoints based on ACLs. Cisco ISE queries the MDM servers for the necessary device attributes to create ACLs that provide network access control for those devices.

You can run multiple active MDM servers on your network, including ones from different vendors. This allows you to route different endpoints to different MDM servers based on device factors such as location or device type.

Cisco ISE also integrates with MDM servers using Cisco’s MDMAPI version 2 to allow devices access the network over VPN via AnyConnect 4.1 and Cisco ASA 9.3.2 or later.

In this illustration, Cisco ISE is the enforcement point and the MDM policy server is the policy information point. Cisco ISE obtains data from the MDM server to provide a complete solution.

You can configure Cisco ISE to interoperate with one or more external Mobile Device Manager (MDM) servers. By setting up this type of third-party connection, you can leverage the detailed information available in the MDM database. Cisco ISE uses REST API calls to retrieve information from the external MDM server. Cisco ISE applies appropriate access control policies to switches, access routers, wireless access points, and other network access points to achieve greater control of remote device access to your Cisco ISE network.

The supported MDM vendors are listed here: Supported MDM Servers, on page 238.
Supported MDM Use Cases

The functions Cisco ISE performs with the external MDM server are as follows:

- Managing device registration—Unregistered endpoints accessing the network are redirected to a registration page, which is hosted on the MDM server. Device registration includes user role, device type, and so on.

- Handling device remediation—Endpoints are granted only restricted access during remediation.

- Augmenting endpoint data—Update the endpoint database with information from the MDM server that you cannot gather using the Cisco ISE Profiler. Cisco ISE uses six device attributes you can view using the Work Centers > Network Access > Identities > Endpoints page if an endpoint is an MDM monitored device. For example:
  
  • MDMImei: 99 000100 160803 3
  • MDMManufacturer: Apple
  • MDMModel: iPhone
  • MDMOSVersion: iOS 6.0.0
  • MDMPhoneNumber: 9783148806
  • MDMSerialNumber: DNPGQZGUDTF9

- Cisco ISE polls the MDM server once every 4 hours for device compliance data. This is configurable by the administrator.

- Issuing device instructions through the MDM server—Issues remote actions for users’ devices through the MDM server. Administrators initiate remote actions from the ISE console.

Vendor MDM Attributes

When you configure an MDM server in ISE, that vendor's attributes are added to a new entry in the ISE system dictionary, named `mdm`. The following attributes are used for registration status, and are commonly supported by MDM vendors.

- DeviceRegisterStatus
- DeviceCompliantStatus
- DiskEncryptionStatus
- PinLockStatus
- JailBrokenStatus
- Manufacturer
- IMEI
- SerialNumber
- OsVersion
- PhoneNumber
Vendor's unique attributes are not supported, but you may be able to use ERS APIs to exchange vendor-specific attributes, if the vendor supports that.

The new MDM dictionary attributes are available to use in authorization policies.

**Supported MDM Servers**

Supported MDM servers include products from the following vendors:

- Absolute
- AirWatch
- Citrix XenMobile
- Globo
- Good Technology
- IBM MaaS360
- JAMF Software
- Meraki SM/EMM
- MobileIron
- SAP Afaria
- SOTI
- Symantec
- Tangoe

- Microsoft Intune - for mobile devices
- Microsoft SCCM - for desktop devices

ISE Community Resource

How To: Meraki EMM / MDM Integration with ISE
Ports Used by the MDM Server

The following table lists the ports that must be open between the Cisco ISE and the MDM server to enable them to communicate with each other. Refer to the MDM Server Documentation for a list of ports that must be open on the MDM agent and server.

Table 11: Ports Used by the MDM Server

<table>
<thead>
<tr>
<th>MDM Server</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>MobileIron</td>
<td>443</td>
</tr>
<tr>
<td>Zenprise</td>
<td>443</td>
</tr>
<tr>
<td>Good</td>
<td>19005</td>
</tr>
<tr>
<td>Airwatch</td>
<td>443</td>
</tr>
<tr>
<td>Afaria</td>
<td>443</td>
</tr>
<tr>
<td>Fiberlink MaaS</td>
<td>443</td>
</tr>
<tr>
<td>Meraki</td>
<td>443</td>
</tr>
<tr>
<td>Microsoft Intune</td>
<td>80 and 443</td>
</tr>
<tr>
<td>Microsoft SCCM</td>
<td>80 and 443</td>
</tr>
</tbody>
</table>

MDM Integration Process Flow

This section describes the MDM integration process:

1. The user associates a device to SSID.
2. Cisco ISE makes an API call to the MDM server.
3. This API call returns a list of devices for this user and the posture status for the devices.

Note

The input parameter is the MAC address of the endpoint device. For off-premise Apple iOS devices, this is the UDID.

4. If the user’s device is not in this list, it means the device is not registered. Cisco ISE sends an authorization request to the NAD to redirect to Cisco ISE. The user is presented the MDM server page.

Note

You must register a device that is enrolled on the MDM server outside of a Cisco ISE network via the MDM portal. This is applicable for Cisco ISE, Release 1.4 and later. Earlier ISE versions allow devices enrolled outside of a Cisco ISE network to be automatically enrolled if they are compliant with the posture policies.
5. Cisco ISE uses MDM to provision the device and presents an appropriate page for the user to register the device.

6. The user registers the device in the MDM server, and the MDM server redirects the request to Cisco ISE (through automatic redirection or manual browser refresh).

7. Cisco ISE queries the MDM server again for the posture status.

8. If the user’s device is not compliant to the posture (compliance) policies configured on the MDM server, the user is notified that the device is out of compliance and must be compliant.

9. After the user’s device becomes compliant, the MDM server updates the device state in its internal tables.

10. If the user refreshes the browser now, the control is transferred back to Cisco ISE.

11. Cisco ISE polls the MDM server once every four hours to get compliance information and issues Change of Authorization (CoA) appropriately. This can be configured by the administrator. Cisco ISE also checks the MDM server every 5 minutes to make sure that it is available.

The following figure illustrates the MDM process flow.

![MDM Process Flow Diagram]

**Note**

A device can only be enrolled to a single MDM server at a time. If you want to enroll the same device to an MDM service from another vendor, the previous vendor’s profiles must be removed from the device. The MDM service usually offers a "corporate wipe", which only deletes the vendor's configuration from the device (not the whole device). The user can also remove the files. For example, on an IOS device, the user can go to Settings > General >Device management, and click remove management. Or the user can go to the MyDevices portal in ISE, and click corporate wipe.

---

**Set Up MDM Servers with Cisco ISE**

To set up MDM servers with Cisco ISE, you must perform the following high-level tasks:

**Step 1** Import MDM server certificate into Cisco ISE, except for Intune, where you import the PAN's certificate into Azure.

**Step 2** Create mobile device manager definitions.
Step 3 Configure ACLs on the Wireless LAN Controllers.
Step 4 Configure an authorization profile that redirects non-registered devices to the MDM server.
Step 5 If there is more than one MDM server on the network, configure separate authorization profiles for each vendor.
Step 6 Configure authorization policy rules for the MDM use cases.

Import MDM Server Certificate into Cisco ISE

For Cisco ISE to connect with the MDM server, you must import the MDM server certificate into the Cisco ISE Certificate Store. If your MDM server has a CA-signed certificate, you must import the root CA into the Cisco ISE Certificate Store.

Note For Microsoft Azure, you import the ISE certificate into Azure. For more information, see Configuring Microsoft Intune as an MDM Server, on page 244.

Step 1 Export the MDM server certificate from your MDM server and save it on your local machine.
Step 2 Choose Administration > System > Certificates > Trusted Certificate > Import.
Step 3 Click Browse to select the MDM server certificate that you obtained from the MDM server.
Step 4 Add a friendly name.
Step 5 Check Trust for authentication within ISE check box.
Step 6 Click Submit.
Step 7 Verify that the Certificate Store list page lists the MDM server certificate.

What to do next
Define Mobile Device Management Servers in ISE, on page 241

Define Mobile Device Management Servers in ISE

You can create one or more Mobile Device Management (MDM) and Desktop Device Manager (SCCM) definitions for external MDM servers.

1. Choose Administration > Network Resources > External MDM.
2. Click Add.
3. Enter the name and description of the MDM server that you want to add.
4. Choose the Server Type, Mobile Device Manager, or Desktop Device Manager. Your choice determines which fields you see next. If you chose Desktop Device Manager, go to Desktop Device Management, on page 243. If you chose Mobile Device Manager, then continue this list of steps.
5. Choose **Authentication Type**, Basic, or OAuth - Client Credentials. If you chose OAuth - Client credentials to configure a Microsoft Intune server, go to Mobile Device Management - OAuth - Client Credentials, on page 242. If you chose Basic, then continue this list of steps.

6. All screens ask for a name and describe this MDM server definition. The following section describes the additional fields and steps, which are based on server and authentication type.

### Mobile Device Management - Basic

- **HostName / IP Address** — Enter the hostname or IP address of the MDM server.
- **Port** — Enter the port to use when connecting to the MDM server, which is usually 443.
- **Instance Name** - If this MDM server has several instances, enter the instance that you want to connect to.
- **Polling Interval** — Enter the polling interval in minutes for Cisco ISE to poll the MDM server for compliance check information. Set this value to match the polling interval on your MDM server. The valid range is from 15 to 1440 minutes. The default value is 240 minutes. We recommend that you set the polling interval below 60 minutes only for testing a few active clients on your network. If you set this value below 60 minutes for a production environment with many active clients, the system’s load increases significantly and may negatively affect performance.

If you set the polling interval to 0, ISE disables communication with the MDM server.

- **TimeIntervalForComplianceDeviceReAuthQuery** — When the endpoint is authenticated or re-authenticated, ISE uses a cache to get the MDM variables for that endpoint. If the age of cached value is older than the value of TimeIntervalForComplianceDeviceReAuthQuery, then ISE makes a device query to the MDM server to get new values. If the compliance status changed, then ISE triggers a CoA. The valid range is from 1 to 1440 minutes. The default value is 1 minute.

### Mobile Device Management - OAuth - Client Credentials

Using OAuth requires configuration of the OAuth server, which is described in Configuring Microsoft Intune as an MDM Server, on page 244.

- **Auto Discovery URL** — Enter the value of **Microsoft Azure AD Graph API Endpoint** from the Microsoft Azure management portal. This URL is the endpoint at which an application can access directory data in your Microsoft Azure AD directory using the Graph API. The URL is of the form:
  
  https://<hostname>/<tenant id>, for example, https://graph.ppe.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329

  An expanded version of this URL is also in the property file, which is of the form:
  
  https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>.

- **Client ID** — The unique identifier for your application. Use this attribute if your application accesses data in another application, such as the Microsoft Azure AD Graph API, Microsoft Intune API, and so on.

- **Token Issuing URL** — Enter the value of the **OAuth2.0 Authorization Endpoint** from the previous step. This is the endpoint at which your app can obtain an access token using OAuth2.0. After your app is authenticated, Microsoft Azure AD issues your app (ISE) an access token, which allows your app to call the Graph API/ Intune API.
• **Token Audience**—The recipient resource that the token is intended for, which is a public, well-known APP ID URL to the Microsoft Intune API.

• **Polling Interval**—Enter the polling interval in minutes for Cisco ISE to poll the MDM server for compliance check information. Set this value to match the polling interval on your MDM server. The valid range is from 15 to 1440 minutes. The default value is 240 minutes. We recommend that you set the polling interval below 60 minutes only for testing a few active clients on your network. If you set this value below 60 minutes for a production environment with many active clients, the system’s load increases significantly and may negatively affect performance.

If you set the polling interval to 0, ISE disables communication with the MDM server.

• **Time Interval For Compliance Device ReAuth Query**—When the endpoint is authenticated or re-authenticated, ISE uses a cache to get the MDM variables for that endpoint. If the age of cached value is older than the value of Time Interval For Compliance Device ReAuth Query, then ISE makes a device query to the MDM server to get new values. If the compliance status changed, then ISE triggers a CoA. The valid range is from 1 to 1440 minutes. The default value is 1 minute.

**Desktop Device Management**

The following settings require you to configure WMI on the SCCM server, so it can communicate with ISE. See Configure the Microsoft SCCM Server for ISE, on page 247 for more information.

• **HostName/IP Address**—Enter the hostname or IP address of the MDM server.

• **Site or Instance Name**—Enter the site name, or if the MDM server has several instances, the instance name.

**ISE MDM Support for Microsoft Intune and SCCM**

• **Microsoft Intune**—MDM-ISE supports Microsoft's Intune device management as a partner MDM server managing mobile devices.

  You configure ISE as an OAuth 2.0 client application on the Intune server managing mobile devices. ISE gets a token from Azure to establish a session with that ISE Intune application.


• **Desktop Device Manager (Microsoft SCCM)** - ISE supports Microsoft's System Center Configuration Manager (SCCM) as a partner MDM server for managing Windows computers. ISE retrieves compliance information from the SCCM server using WMI, and uses that information to grant or deny network access to the user's Windows device.

**SCCM Workflow**

ISE is able to retrieve information from the SCCM server about whether a device is registered, and if it is registered, is it compliant. The following diagram shows the workflow for devices managed by SCCM.
When a device connects and a SCCM policy is matched, ISE queries the SCCM server specified in the authorization policy to retrieve compliance and last logon (check-in) time. With this information, ISE updates the compliance status and lastCheckinTimeStamp of the device in the Endpoint list.

If the device is not compliant or not registered with SCCM, and a redirect profile is used in the authorization policy, a message is displayed to the user that the device is not compliant or not registered with the SCCM. After the user acknowledges the message, ISE can issue a CoA to the SCCM registration site. Users can be granted access based on the authorization policy and profile.

**Microsoft SCCM Server Connection Monitoring**

Polling is not configurable for SCCM.

ISE runs an MDM HeartBeat job that verifies connection to the SCCM server, and raises alarms if ISE loses the connection to the SCCM server. The HeartBeat job interval is not configurable.

**Configuring Microsoft Intune as an MDM Server**

Configuring Microsoft Intune as an MDM server for ISE is slightly differently from configuring other MDM servers. Use the following steps to configure ISE's connection to Azure and Azure's connection to ISE.

1. Get the public certificate from the Intune/Azure Active Directory tenant, and import it into ISE to support SSL handshake.
   1. 1. Log on to the Intune Admin Console or Azure Admin console, whichever site has your tenant.
   2. Use the browser to get the certificate details. For, example, with Internet Explorer:
      1. Click on the lock symbol in the browsers toolbar, then click View Certificates.
      2. In the Certificate window, select the tab Certification Path.
      3. Find Baltimore Cyber Trust root, and export the root cert.
   3. In ISE, choose Administration > System > Certificates > Trusted Certificates, and import the root certificate that you just saved. Give the certificate a meaningful name, such as Azure MDM.
2. Export the ISE self-signed certificate, and prepare it for InTune/Azure.

   1. On the PAN, navigate to Administration > System > Certificates > System Certificates, select the Default self-signed server certificate, and click Export.

   2. Select Export Certificate Only (default), and select a place to save it.

   Run the following PowerShell script on the exported certificate file:

   ```powershell
   $cer.Import("mycer.cer")
   $bin = $cer.GetRawCertData()
   $base64Value = [System.Convert]::ToBase64String($bin)
   $bin = $cer.GetCertHash()
   $base64Thumbprint = [System.Convert]::ToBase64String($bin)
   $keyid = [System.Guid]::NewGuid().ToString()
   
   Keep the values for $base64Thumbprint, $base64Value and $keyid, which will be used in the next step.

3. Create an ISE application in Intune.

   1. Sign in to your customer domain on the Microsoft Azure management portal, navigate to Directory > Applications > Add an Application, and choose Add an application my organization is developing.

   2. Configure the ISE application in Azure with the following parameters:

      • **Application Name**— enter ISE.

      • Select WEB APPLICATION AND/OR WEB APP.

      • **SIGN-ON URL and APP ID URL**— Add any valid URL, these values are not used by ISE.

4. Get the manifest file from Azure, add the ISE certificate information, and upload the updated manifest into Azure.

   1. On the Microsoft Azure management portal ([https://manage.windowsazure.com](https://manage.windowsazure.com)), open the AAD snap-in, and navigate to the ISE application.

   Download the application manifest file from the **Manage Manifest** menu.

5. Update the **keyCredentials** field in Manifest json file as shown in the following example, replacing Base64 Encoded String of ISE PAN cert with the exported, edited, certificate file from ISE, which is the $base64Value from the PowerShell script:

   ```json
   "keyCredentials": [
     {
       "customKeyIdentifier": "$base64Thumbprint_from_above",
       "keyId": "$keyid_from_above",
       "type": "AsymmetricX509Cert",
       "usage": "Verify",
       "value": "Base64 Encoded String of ISE PAN cert"
     }
   ]
   ```

   **Note**

   Do not change the name of the manifest file.
The KeyCredentials complex type is documented here:

6. Upload the updated manifest file to Azure.

7. On the Microsoft Azure management portal, navigate to the list of App Endpoints. You will use the values of following endpoint attributes to configure ISE:
   - MICROSOFT AZURE AD GRAPH API ENDPOINT
   - OAUTH 2.0 TOKEN ENDPOINT

8. In ISE, configure the Intune server in ISE. For more information about configuring and external MDM server, see Define Mobile Device Management Servers in ISE, on page 241. The fields that are important for Intune are described below:

   • **Auto Discovery URL**—Enter the value of *Microsoft Azure AD Graph API Endpoint* from the Microsoft Azure management portal. This URL is the endpoint at which an application can access directory data in your Microsoft Azure AD directory using the Graph API. The URL is of the form:
     https://<hostname>/<tenant id>, for example, https://graph.ppe.windows.net/47f09275-5bc0-4807-8aae-f35cb0341329. An expanded version of this URL is also in the property file, which is of the form:
     https://<Graph_API_Endpoint>/<TenantId_Or_Domain>/servicePrincipalsByAppId/<Microsoft Intune AppId>/serviceEndpoints?api-version=1.6&client-request-id=<Guid.NewGuid()>.

   • **Client ID**—The unique identifier for your application. Use this attribute if your application accesses data in another application, such as the Microsoft Azure AD Graph API, Microsoft Intune API, and so on.

   • **Token Issuing URL**—Enter the value of the *Oauth2.0 Authorization Endpoint* from the previous step. This is the endpoint at which your app can obtain an access token using OAuth2.0. After your app is authenticated, Microsoft Azure AD issues your app (ISE) an access token, which allows your app to call the Graph API/Intune API.

   • **Token Audience**—The recipient resource that the token is intended for, which is a public, well-known APP ID URL to the Microsoft Intune API.

For more information about Intune applications, see the following links:


**Policy Set Example for Microsoft SCCM**

The following new dictionary entries can be used in policies to support SCCM.

- MDM.DaysSinceLastCheckin - Number of days since a user last checked in or synched a device with SCCM, from 1 to 365 days.
- MDM.UserNotified - Values are Y or N. Indicates whether the user was notified that they are not registered. You can then allow limited access and redirect to registration portal, or deny access.
- MDM.ServerType - Values are MDM for Mobile Device Manager or DM for Desktop Device Manager.

The following example Policy Set shows a set of policies to support SCCM:

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCCM_Compliant</td>
<td>PermitAccessWireless_802.1X AND MDM:MDMServerName EQUALS ScmServer1 AND MDM:DeviceRegisterStatus EQUALS Registered</td>
</tr>
<tr>
<td>SCCM_NonComp_UsrNoti_yes</td>
<td>PermitAccessWireless_802.1X AND MDM:MDMServerName EQUALS ScmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:UserNotified EQUALS 28</td>
</tr>
<tr>
<td>SCCM_NonCompliant_DaysSince</td>
<td>SCCM_RedirectWireless_802.1X AND MDM:MDMServerName EQUALS ScmServer1 AND MDM:MDMDeviceCompliantStatus EQUALS Registered AND MDM:DaysSinceLastCheckin EQUALS 28</td>
</tr>
<tr>
<td>SCCM_NonCompliant</td>
<td>SCCM_RedirectWireless_802.1X AND MDM:MDMServerName EQUALS ScmServer1 AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:DeviceRegisterStatus EQUALS Registered</td>
</tr>
<tr>
<td>SCCM_UnReg_UsrNotified_Yes</td>
<td>PermitAccessWireless_802.1X AND MDM:DeviceRegisterStatus EQUALS Registered AND MDM:UserNotified EQUALS Yes</td>
</tr>
</tbody>
</table>

**Configure the Microsoft SCCM Server for ISE**

ISE communicates with the SCCM server using WMI. WMI must be configured on the Windows server running SCCM.
The user account that you use for ISE integration must either:

- Be a member of SMSAdmins user group.
- Have the same permissions as the SMS object under the WMI namespace

\[ \text{root}\sms\site_{\text{sitecode}} \]

where sitecode is the SCCM site.

**Set Permissions When AD User in the Domain Admin Group**

For Windows 2008 R2, Windows 2012, and Windows 2012 R2, the Domain Admin group does not have full control on certain registry keys in the Windows operating system by default. The Active Directory admin must give the Active Directory user Full Control permissions on the following registry keys:

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

No registry changes are required for the following Active Directory versions:

- Windows 2003
- Windows 2003 R2
- Windows 2008

To grant full control, the Active Directory admin must first take ownership of the key, as shown below.

**Step 1**
Go to the Owner tab by right clicking the key.

**Step 2**
Click Permissions.

**Step 3**
Click Advanced.

**Required Permissions when AD User not in Domain Admin Group**

For Windows 2012 R2, give the Active Directory user **Full Control** permissions on the following registry keys:

- **HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**
- **HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}**

The following permissions also are required when an Active Directory user is not in the Domain Admin group, but is in the Domain Users group:

- Add Registry Keys to Allow ISE to Connect to the Domain Controller (see below)
- Permissions to Use DCOM on the Domain Controller, on page 249
- Set Permissions for Access to WMI Root/CIMv2 Name Space, on page 251
These permissions are only required for the following Active Directory versions:

- Windows 2003
- Windows 2003 R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

**Add Registry Keys to Allow ISE to Connect to the Domain Controller**

You must manually add some registry keys to the domain controller to allow ISE to connect as a Domain User, and retrieve login authentication events. An agent is not required on the domain controllers or on any machine in the domain.

The following registry script shows the keys to add. You can copy and paste this into a text file, save the file with a .reg extension, and double click the file to make the registry changes. To add registry keys, the user must be an owner of the root key.

```
Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" "

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=" "
```

Make sure that you include two spaces in the value of the key DllSurrogate.

Keep the empty lines as shown in the script above, including an empty line at the end of the file.

**Permissions to Use DCOM on the Domain Controller**

The Active Directory user used for ISE Passive Identity services must have permissions to use DCOM (remote COM) on the Domain Controller. You can configure permissions with the dcomcnfg command line tool.

**Step 1** Run the dcomcnfg tool from the command line.

**Step 2** Expand **Component Services**.

**Step 3** Expand **Computers > My Computer**.

**Step 4** Select Action from the menu bar, click **properties**, and click **COM Security**.

**Step 5** Make sure that the account that ISE will use for both Access and Launch has Allow permissions. That Active Directory user should be added to all the four options (Edit Limits and Edit Default for both Access Permissions and Launch and Activation Permissions).

**Step 6** Allow all Local and Remote access for both Access Permissions and Launch and Activation Permissions.
Setup Cisco ISE Management Access

Permissions to Use DCOM on the Domain Controller

Figure 13: Local and Remote Access for Access Permissions

![Diagram showing Local and Remote Access for Access Permissions](image-url)

Learn about access control and permissions

OK Cancel
Set Permissions for Access to WMI Root/CIMv2 Name Space

By default, Active Directory users do not have permissions for the Execute Methods and Remote Enable. You can grant access using the wmiimgmt.msc MMC console.

**Step 1**  Click Start > Run and type `wmiimgmt.msc`.
**Step 2**  Right-click WMI Control and click **Properties**.
**Step 3**  Under the Security tab, expand Root and choose **CIMV2**.
**Step 4**  Click **Security**.
**Step 5**  Add the Active Directory user, and configure the required permissions as shown below.
Set Permissions When AD User in the Domain Admin Group

For Windows 2008 R2, Windows 2012, and Windows 2012 R2, the Domain Admin group does not have full control on certain registry keys in the Windows operating system by default. The Active Directory admin must give the Active Directory user Full Control permissions on the following registry keys:

- HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
- HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

No registry changes are required for the following Active Directory versions:

- Windows 2003
- Windows 2003R2
- Windows 2008
To grant full control, the Active Directory admin must first take ownership of the key, as shown below.

**Step 1** Go to the Owner tab by right clicking the key.
**Step 2** Click Permissions.
**Step 3** Click Advanced.

### Required Permissions when AD User not in Domain Admin Group

For Windows 2012 R2, give the Active Directory user **Full Control** permissions on the following registry keys:

- HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
- HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

The following permissions also are required when an Active Directory user is not in the Domain Admin group, but is in the Domain Users group:

- Add Registry Keys to Allow ISE to Connect to the Domain Controller (see below)
- Permissions to Use DCOM on the Domain Controller, on page 249
- Set Permissions for Access to WMI Root/CIMv2 Name Space, on page 251

These permissions are only required for the following Active Directory versions:

- Windows 2003
- Windows 2003 R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

**Add Registry Keys to Allow ISE to Connect to the Domain Controller**

You must manually add some registry keys to the domain controller to allow ISE to connect as a Domain User, and retrieve login authentication events. An agent is not required on the domain controllers or on any machine in the domain.

The following registry script shows the keys to add. You can copy and paste this into a text file, save the file with a .reg extension, and double click the file to make the registry changes. To add registry keys, the user must be an owner of the root key.

**Windows Registry Editor Version 5.00**

```
[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"
```

Make sure that you include two spaces in the value of the key **DllSurrogate**.

Keep the empty lines as shown in the script above, including an empty line at the end of the file.

**Permissions to Use DCOM on the Domain Controller**

The Active Directory user used for ISE Passive Identity services must have permissions to use DCOM (remote COM) on the Domain Controller. You can configure permissions with the **dcomcnfg** command line tool.

---

**Step 1** Run the **dcomcnfg** tool from the command line.

**Step 2** Expand **Component Services**.

**Step 3** Expand **Computers > My Computer**.

**Step 4** Select Action from the menu bar, click **properties**, and click **COM Security**.

**Step 5** Make sure that the account that ISE will use for both Access and Launch has Allow permissions. That Active Directory user should be added to all the four options (Edit Limits and Edit Default for both Access Permissions and Launch and Activation Permissions).

**Step 6** Allow all Local and Remote access for both Access Permissions and Launch and Activation Permissions.

*Figure 16: Local and Remote Access for Access Permissions*
**Set Permissions for Access to WMI Root/CIMv2 Name Space**

By default, Active Directory users do not have permissions for the Execute Methods and Remote Enable. You can grant access using the wmingmt.msc MMC console.

**Step 1**
Click Start > Run and type `wmingmt.msc`.

**Step 2**
Right-click WMI Control and click **Properties**.

**Step 3**
Under the Security tab, expand Root and choose CIMV2.

**Step 4**
Click **Security**.

**Step 5**
Add the Active Directory user, and configure the required permissions as shown below.
Open Firewall Ports for WMI Access

The firewall software on the Active Directory Domain Controller may block access to WMI. You can either turn the firewall off, or allow access on a specific IP (ISE IP address) to the following ports:

- TCP 135: General RPC Port. When doing asynchronous RPC calls, the service listening on this port tells the client which port the component servicing this request is using.
- UDP 138: Netbios Datagram Service
- TCP 139: Netbios Session Service
- TCP 445: SMB

**Note**

Cisco ISE 1.3 and above support SMB 2.0.
Higher ports are assigned dynamically or you can configure them manually. We recommend that you add %SystemRoot%\System32\dllhost.exe as a target. This program manages ports dynamically.

All firewall rules can be assigned to specific IP (ISE IP).

**Configure an Authorization Profile for Redirecting Nonregistered Devices**

You must configure an authorization profile in Cisco ISE to redirect nonregistered devices for each external MDM server.

**Before you begin**

- Ensure that you have created an MDM server definition in Cisco ISE. Only after you successfully integrate ISE with the MDM server does the MDM dictionary get populated and you can create authorization policy using the MDM dictionary attributes.
- Configure ACLs on the Wireless LAN Controller for redirecting unregistered devices.
- If you are using a proxy for the internet connection and MDM server is part of internal network then you have to put the MDM server name or its IP address in the Proxy-Bypass list. Choose Administration > Settings > Proxy Settings to perform this action.

**Step 1** Choose Policy > Policy Elements > Results > Authorization > Authorization Profiles > Add.
**Step 2** Create an authorization profile for redirecting nonregistered devices that are not compliant or registered.
**Step 3** Enter a name for the authorization profile that matches the MDM server name.
**Step 4** Choose ACCESS_ACCEPT as the Access Type.
**Step 5** Check the Web Redirection check box and choose MDM Redirect from the drop-down list.
**Step 6** Enter the name of the ACL that you configured on the wireless LAN controller in the ACL field.
**Step 7** Select the MDM portal from the Value drop-down list.
**Step 8** Select the MDM server you want to use from the drop-down list.
**Step 9** Click Submit.

**What to do next**

Configure Authorization Policy Rules for the MDM Use Cases.

**Configure Authorization Policy Rules for the MDM Use Cases**

You must configure authorization policy rules in Cisco ISE to complete the MDM configuration.

**Before you begin**

- Add the MDM server certificate to the Cisco ISE certificate store.
- Ensure that you have created the MDM server definition in Cisco ISE. Only after you successfully integrate ISE with the MDM server, the MDM dictionary gets populated and you can create authorization policy using the MDM dictionary attributes.
- Configure ACLs on the Wireless LAN Controller for redirecting unregistered or noncompliant devices.
Step 1  Choose **Policy** > **Policy Sets**, and expand the policy set to view the authorization policy rules.

Step 2  Add the following rules:

- **MDM_Un_Registered_Non_Compliant**—For devices that are not yet registered with an MDM server or compliant with MDM policies. Once a request matches this rule, the ISE MDM page appears with information on registering the device with MDM.

- **PERMIT**—If the device is registered with Cisco ISE, registered with MDM, and is compliant with Cisco ISE and MDM policies, it will be granted access to the network based on the access control policies configured in Cisco ISE.

The following illustration shows an example of this configuration.

*Figure 19: Authorization Policy Rules for the MDM Use Cases*

![Image of policy rules](image)

Step 3  Click **Save**.

---

**Wipe or Lock a Device**

Cisco ISE allows you to wipe or turn on pin lock for a device that is lost. You can do this from the Endpoints page.

**Step 1**  Choose **Work Centers > Network Access > Identities > Endpoints**.

**Step 2**  Check the check box next to the device that you want to wipe or lock.

**Step 3**  From the MDM Access drop-down list, choose any one of the following options:

- **Full Wipe**—Depending on the MDM vendor, this option either removes the corporate apps or resets the device to the factory settings.

- **Corporate Wipe**—Removes applications that you have configured in the MDM server policies

- **PIN Lock**—Locks the device

**Step 4**  Click **Yes** to wipe or lock the device.

---

**View Mobile Device Manager Reports**

Cisco ISE records all additions, updates, and deletions of MDM server definitions. You can view these event in the “Change Configuration Audit” report, which provides all the configuration changes from any system administrator for a selected time period.
Choose Operations > Reports > Change Configuration Audit > MDM, and specify the period of time to display in the resulting report.

View Mobile Device Manager Logs

You can use the Message Catalog page to view Mobile Device Manager log messages. Choose Administration > System > Logging > Message Catalog. The default reporting level for MDM log entries is "INFO." You can change the reporting level to "DEBUB" or "TRACE."
CHAPTER 11

Manage Resources

- Dictionaries and Dictionary Attributes, on page 261
- RADIUS-Vendor Dictionaries, on page 263

Dictionaries and Dictionary Attributes

Dictionaries are domain-specific catalogs of attributes and allowed values that can be used to define access policies for a domain. An individual dictionary is a homogeneous collection of attribute type. Attributes that are defined in a dictionary have the same attribute type and the type indicates the source or context of a given attribute.

Attribute types can be one of the following:

- MSG_ATTR
- ENTITY_ATTR
- PIP_ATTR

In addition to attributes and allowed values, a dictionary contains information about the attributes such as the name and description, data type, and the default values. An attribute can have one of the following data types: BOOLEAN, FLOAT, INTEGER, IPv4, IPv6, OCTET_STRING, STRING, UNIT32, and UNIT64.

Cisco ISE creates system dictionaries during installation and allows you to create user dictionaries.

System Defined Dictionaries and Dictionary Attributes

Cisco ISE creates system dictionaries during installation that you can find in the System Dictionaries page. System-defined dictionary attributes are read-only attributes. Because of their nature, you can only view existing system-defined dictionaries. You cannot create, edit, or delete system-defined values or any attributes in a system dictionary.

A system-defined dictionary attribute is displayed with the descriptive name of the attribute, an internal name as understood by the domain, and allowed values.

Cisco ISE also creates dictionary defaults for the IETF RADIUS set of attributes that are also a part of the system-defined dictionaries, which are defined by the Internet Engineering Task Force (IETF). You can edit all free IETF RADIUS attribute fields except the ID.
Display System Dictionaries and Dictionary Attributes

You cannot create, edit, or delete any system-defined attribute in a system dictionary. You can only view system-defined attributes. You can perform a quick search that is based on a dictionary name and description or an advanced search that is based on a search rule that you define.

Step 1  Choose Policy > Policy Elements > Dictionaries > System.
Step 2  Choose a system dictionary in the System Dictionaries page, and click View.
Step 3  Click Dictionary Attributes.
Step 4  Choose a system dictionary attribute from the list, and click View.
Step 5  Click the Dictionaries link to return to the System Dictionaries page.

User-Defined Dictionaries and Dictionary Attributes

Cisco ISE displays the user-defined dictionaries that you create in the User Dictionaries page. You cannot modify the values for Dictionary Name or Dictionary Type for an existing user dictionary once created and saved in the system.

You can do the following in the User Dictionaries page:

• Edit and delete user dictionaries.
• Search user dictionaries based on name and description.
• Add, edit, and delete user-defined dictionary attributes in the user dictionaries.
• Delete attributes of the NMAP extension dictionary, using the NMAP scan action. When custom ports are added or deleted in the NMAP Scan Actions page, the corresponding custom ports attributes are added, deleted, or updated in the dictionary.
• Add or remove allowed values for dictionary attributes.

Create User-Defined Dictionaries

You can create, edit, or delete user-defined dictionaries.
Create User-Defined Dictionary Attributes

You can add, edit, and delete user-defined dictionary attributes in user dictionaries as well as add or remove allowed values for the dictionary attributes.

Step 1
Choose Policy > Policy Elements > Dictionaries > User.

Step 2
Choose a user dictionary from the User Dictionaries page, and click Edit.

Step 3
Click Dictionary Attributes.

Step 4
Click Add.

Step 5
Enter the name for an attribute name, an optional description, and an internal name for the dictionary attribute.

Step 6
Choose a data type from the Data Type drop-down list.

Step 7
Click Add to configure the name, allowed value, and set the default status in the Allowed Values table.

Step 8
Click Submit.

RADIUS-Vendor Dictionaries

Cisco ISE allows you to define a set of RADIUS-vendor dictionaries, and define a set of attributes for each one. Each vendor definition in the list contains the vendor name, the vendor ID, and a brief description.

Cisco ISE provides you the following RADIUS-vendor dictionaries by default:

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft

The RADIUS protocol supports these vendor dictionaries, and the vendor-specific attributes that can be used in authorization profiles and in policy conditions.

Related Topics
- Create RADIUS-Vendor Dictionaries, on page 264
- Create RADIUS-Vendor Dictionary Attributes, on page 264
Create RADIUS-Vendor Dictionaries

You can also create, edit, delete, export, and import RADIUS-vendor dictionaries.

Step 1 Choose Policy > Policy Elements > Dictionaries > System > Radius > Radius Vendors.
Step 2 Click Add.
Step 3 Enter a name for the RADIUS-vendor dictionary, an optional description, and the vendor ID as approved by the Internet Assigned Numbers Authority (IANA) for the RADIUS vendor.
Step 4 Choose the number of bytes taken from the attribute value to specify the attribute type from the Vendor Attribute Type Field Length drop-down list. Valid values are 1, 2, and 4. The default value is 1.
Step 5 Choose the number of bytes taken from the attribute value to specify the attribute length from the Vendor Attribute Size Field Length drop-down list. Valid values are 0 and 1. The default value is 1.
Step 6 Click Submit.

Related Topics
Create RADIUS-Vendor Dictionary Attributes, on page 264

Create RADIUS-Vendor Dictionary Attributes

You can create, edit, and delete RADIUS vendor attributes that Cisco ISE supports. Each RADIUS-vendor attribute has a name, data type, description, and direction, which specifies whether it is relevant to requests only, responses only, or both.

Step 1 Choose Policy > Policy Elements > Dictionaries > System > Radius > Radius Vendors.
Step 2 Choose a RADIUS-vendor dictionary from the RADIUS vendor dictionaries list, and click Edit.
Step 3 Click Dictionary Attributes, and then click Add.
Step 4 Enter the attribute name for the RADIUS vendor attribute and an optional description.
Step 5 Choose the data type from the Data Type drop-down list.
Step 6 Check the Enable MAC option check box.
Step 7 Choose the direction that applies to RADIUS requests only, RADIUS responses only, or both from the Direction drop-down list.
Step 8 Enter the vendor attribute ID in the ID field.
Step 9 Check the Allow Tagging check box.
Step 10 Check the Allow multiple instances of this attribute in a profile check box.
Step 11 Click Add to add the allowed value for the vendor attribute in the Allowed Values table.
Step 12 Click Submit.

HP RADIUS IETF Service Type Attributes

Cisco ISE introduces two new values for the RADIUS IETF Service Type attribute. The RADIUS IETF service type attribute is available in Policy > Policy Elements > Dictionaries > System > RADIUS > IETF.
You can use these two values in policy conditions. These two values are specifically designed for HP devices to understand permissions of the user.

<table>
<thead>
<tr>
<th>Enumeration Name</th>
<th>Enumeration Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP-Oper</td>
<td>252</td>
</tr>
<tr>
<td>HP-User</td>
<td>255</td>
</tr>
</tbody>
</table>
CHAPTER 12

Logging Mechanism

• Cisco ISE Logging Mechanism, on page 267
• Cisco ISE System Logs, on page 268
• Configure Remote Syslog Collection Locations, on page 272
• Cisco ISE Message Codes, on page 273
• Cisco ISE Message Catalogs, on page 274
• Debug Logs, on page 274
• Endpoint Debug Log Collector, on page 275
• Collection Filters, on page 276

Cisco ISE Logging Mechanism

Cisco ISE provides a logging mechanism that is used for auditing, fault management, and troubleshooting. The logging mechanism helps you to identify fault conditions in deployed services and troubleshoot issues efficiently. It also produces logging output from the monitoring and troubleshooting primary node in a consistent fashion.

You can configure a Cisco ISE node to collect the logs in the local systems using a virtual loopback address. To collect logs externally, you configure external syslog servers, which are called targets. Logs are classified into various predefined categories. You can customize logging output by editing the categories with respect to their targets, severity level, and so on.

Configuring network devices to send sylogs into the ISE MnT node is not a best practice as this could result in the loss of some NAD sylogs. Only ISE should be sending updates to the MnT node.

**Note**

If the Monitoring node is configured as the syslog server for a network device, ensure that the logging source sends the correct network access server (NAS) IP address in the following format:

\(<message_number>\);sequence_number: NAS_IP_address: timestamp: syslog_type: <message_text>

Otherwise, this might impact functionalities that depend on the NAS IP address.

Configure Local Log Purge Settings

Use this process to set local log-storage periods and to delete local logs after a certain period of time.
Step 1  Choose Administration > System > Logging > Local Log Settings.
Step 2  In the Local Log Storage Period field, enter the maximum number of days to keep the log entries in the configuration source.
Step 3  Click Delete Logs Now to delete the existing log files at any time before the expiration of the storage period.
Step 4  Click Save.

Cisco ISE System Logs

In Cisco ISE, system logs are collected at locations called logging targets. Targets refer to the IP addresses of the servers that collect and store logs. You can generate and store logs locally, or you can use the FTP facility to transfer them to an external server. Cisco ISE has the following default targets, which are dynamically configured in the loopback addresses of the local system:

- LogCollector—Default syslog target for the Log Collector.
- ProfilerRadiusProbe—Default syslog target for the Profiler Radius Probe.

By default, AAA Diagnostics subcategories and System Diagnostics subcategories logging targets are disabled during a fresh Cisco ISE installation or an upgrade to reduce the disk space. You can configure logging targets manually for these subcategories but local logging for these subcategories are always enabled.

You can use the default logging targets that are configured locally at the end of the Cisco ISE installation or you can create external targets to store the logs.

Note  If a syslog server is configured in a distributed deployment, syslog messages are sent directly from the authenticating PSNs to the syslog server and not from the MnT node.

Related Topics
  Cisco ISE Message Codes, on page 273

Local Store Syslog Message Format

Log messages are sent to the local store with this syslog message format:

\[ \text{timestamp sequence_num msg_ode msg_sev msg_class msg_text attr =value} \]
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timestamp</td>
<td>Date of the message generation, according to the local clock of the originating the Cisco ISE node, in the following format: YYYY-MM-DD hh:mm:ss:xxx +/-zh:zm. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• YYYY = Numeric representation of the year.</td>
</tr>
<tr>
<td></td>
<td>• MM = Numeric representation of the month. For single-digit months (1 to 9) a zero precedes the number.</td>
</tr>
<tr>
<td></td>
<td>• DD = Numeric representation of the day of the month. For single-digit days (1 to 9), a zero precedes the number.</td>
</tr>
<tr>
<td></td>
<td>• hh = The hour of the day—00 to 23.</td>
</tr>
<tr>
<td></td>
<td>• mm = The minute of the hour—00 to 59.</td>
</tr>
<tr>
<td></td>
<td>• ss = The second of the minute—00 to 59.</td>
</tr>
<tr>
<td></td>
<td>• xxx = The millisecond of the second—000 to 999.</td>
</tr>
<tr>
<td></td>
<td>• +/-zh:zm = The time zone offset from the Cisco ISE server’s time zone, where zh is the number of offset hours and zm is the number of minutes of the offset hour, all of which is preceded by a minus or plus sign to indicate the direction of the offset. For example, +02:00 indicates that the message occurred at the time indicated by the timestamp, and on a Cisco ISE node that is two hours ahead of the Cisco ISE server’s time zone.</td>
</tr>
<tr>
<td>sequence_num</td>
<td>Global counter of each message. If one message is sent to the local store and the next to the syslog server target, the counter increments by 2. Possible values are 0000000001 to 9999999999.</td>
</tr>
</tbody>
</table>
Remote Syslog Message Format

You can use the web interface to configure logging category messages so that they are sent to remote syslog server targets. Log messages are sent to the remote syslog server targets in accordance with the syslog protocol standard (see RFC-3164). The syslog protocol is an unsecure UDP.

A message is generated when an event occurs. An event may be one that displays a status, such as a message displayed when exiting a program, or an alarm. There are different types of event messages generated from different facilities such as the kernel, mail, user level, and so on. An event message is associated with a severity level, which allows an administrator to filter the messages and prioritize it. Numerical codes are assigned to the facility and the severity level. A Syslog server is an event message collector and collects event messages from these facilities. The administrator can select the event message collector to which messages will be forwarded based upon their severity level. Refer to the Logging Category Settings section for the severity levels in Cisco ISE.

Log messages are sent to the remote syslog server with this syslog message header format, which precedes the local store syslog message format:

```
pri_num Mmm DD hh:mm:ss:xx:xx:xx/host_name cat_name msg_id total_seg seg_num
```

### Field Description

<p>| attr=value | Set of attribute-value pairs that provides details about the logged event. A comma (,) separates each pair. Attribute names are as defined in the Cisco ISE dictionaries. Values of the Response direction AttributesSet are bundled to one attribute called Response and are enclosed in curly brackets {}. In addition, the attribute-value pairs within the Response are separated by semicolons. For example, Response={RadiusPacketType=AccessAccept; AuthenticationResult=UnknownUser; cisco-av-pair=sga:security-group-tag=0000-00;} |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| pri_num | Priority value of the message; a combination of the facility value and the severity value of the message. Priority value = (facility value * 8) + severity value. See Set Severity Levels for Message Codes for security levels. The facility code valid options are:  
  - LOCAL0 (Code = 16)  
  - LOCAL1 (Code = 17)  
  - LOCAL2 (Code = 18)  
  - LOCAL3 (Code = 19)  
  - LOCAL4 (Code = 20)  
  - LOCAL5 (Code = 21)  
  - LOCAL6 (Code = 22; default)  
  - LOCAL7 (Code = 23) |
| time   | Date of the message generation, according to the local clock of the originating Cisco ISE server, in the format Mmm DD hh:mm:ss. Possible values are:  
  - DD = Numeric representation of the day of the month. For single-digit days (1 to 9), a space precedes the number.  
  - hh = The hour of the day—00 to 23.  
  - mm = The minute of the hour—00 to 59.  
  - ss = The second of the minute—00 to 59.  
Some devices send messages that specify a time zone in the format +/-hhmm, where - and + identifies the directional offset from the Cisco ISE server’s time zone, hh is the number of offset hours, and mm is the number of minutes of the offset hour. For example, +02:00 indicates that the message occurred at the time indicated by the time stamp, and on a Cisco ISE node that is two hours ahead of the Cisco ISE server’s time zone. |
Configure Remote Syslog Collection Locations

You can create external locations to store the syslogs.

The UDP SysLog (Log Collector) is the default remote logging target. When you disable this logging target, it no longer functions as a log collector and is removed from the Logging Categories page. When you enable this logging target, it becomes a log collector in the Logging Categories page.

**Step 1** Choose Administration > System > Logging > Remote Logging Targets.

**Step 2** Click Add.

**Step 3** Enter the required details.

**Step 4** Click Save.

**Step 5** Go to the Remote Logging Targets page and verify the creation of the new target.

The logging targets can then be mapped to each of the logging categories below. The PSN nodes send the relevant logs to the remote logging targets depending on the services that are enabled on those nodes.

- AAA Audit
- AAA Diagnostics
- Accounting
- External MDM

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>xx:xx:xx:xx/host_name</td>
<td>IP address of the originating Cisco ISE node, or the hostname.</td>
</tr>
<tr>
<td>cat_name</td>
<td>Logging category name preceded by the CSCOxxx string.</td>
</tr>
<tr>
<td>msg_id</td>
<td>Unique message ID; 1 to 4294967295. The message ID increases by 1 with each new message. Message IDs restart at 1 each time the application is restarted.</td>
</tr>
<tr>
<td>total_seg</td>
<td>Total number of segments in a log message. Long messages are divided into more than one segment. <strong>Note</strong> The total_seg depends on the Maximum Length setting in the remote logging targets page. See Remote Logging Target Settings.</td>
</tr>
<tr>
<td>seg_num</td>
<td>Segment sequence number within a message. Use this number to determine what segment of the message you are viewing.</td>
</tr>
</tbody>
</table>
• Passive ID
• Posture and Client Provisioning Audit
• Posture and Client Provisioning Diagnostics
• Profiler

Logs of the following categories are sent by all nodes in the deployment to the logging targets:
• Administrative and Operational Audit
• System Diagnostics
• System Statistics

Cisco ISE Message Codes

A logging category is a bundle of message codes that describe a function, a flow, or a use case. In Cisco ISE, each log is associated with a message code that is bundled with the logging categories according to the log message content. Logging categories help describe the content of the messages that they contain.

Logging categories promote logging configuration. Each category has a name, target, and severity level that you can set, as per your application requirement.

Cisco ISE provides predefined logging categories for services, such as Posture, Profiler, Guest, AAA (authentication, authorization, and accounting), and so on, to which you can assign log targets.

Related Topics
Set Severity Levels for Message Codes, on page 273

Set Severity Levels for Message Codes

You can set the log severity level and choose logging targets where the logs of selected categories will be stored.

Step 1 Choose Administration > System > Logging > Logging Categories.
Step 2 Click the radio button next to the category that you want to edit, and click Edit.
Step 3 Modify the required field values.
Step 4 Click Save.
Step 5 Go to the Logging Categories page and verify the configuration changes that were made to the specific category.
Cisco ISE Message Catalogs

You can use the Message Catalog page to view all possible log messages and the descriptions. Choose Administration > System > Logging > Message Catalog.

The Log Message Catalog page appears, from which you can view all possible log messages that can appear in your log files. Choose Export to export all the syslog messages in the form of a CSV file.

Debug Logs

Debug logs capture bootstrap, application configuration, runtime, deployment, monitoring, reporting, and public key infrastructure (PKI) information. Critical and warning alarms for the past 30 days and info alarms for the past 7 days are included in the debug logs.

You can configure the debug log severity level for individual components.

You can use the Reset to Default option for a node or component to reset the log level back to factory-shipped default values.

You can store the debug logs in the local server.

---

Note

Debug log configuration is not saved when a system is restored from a backup or upgraded.

Related Topics

Configure Debug Log Severity Level, on page 274

View Logging Components for a Node

Step 1  Choose Administration > System > Logging > Debug Log Configuration.

Step 2  Select the node for which you want to view the logging components, and then click Edit.

The Debug Level Configuration page appears. You can view the following details:

• List of logging components based on the services that are running on the selected node
• Description for each component
• Current log level that is set for the individual components

Configure Debug Log Severity Level

You can configure the severity levels for the debug logs.

Step 1  Choose Administration > System > Logging > Debug Log Configuration.
Step 2  Select the node, and then click **Edit**.

The Debug Log Configuration page displays a list of components based on the services that are running in the selected node and the current log level that is set for the individual components. You can use the **Reset to Default** option for a node or component to reset the log level back to factory-shipped default values.

Step 3  Select the component for which you want to configure the log severity level, and then click **Edit**. Choose the desired log severity level from the **Log Level** drop-down list, and click **Save**.

**Note**  Changing the log severity level of the runtime-AAA component changes the log level of its subcomponent prrt-JNI as well. A change in subcomponent log level does not affect its parent component.

## Endpoint Debug Log Collector

To troubleshoot issues with a specific endpoint, you can download debug logs for that particular endpoint based on its IP address or MAC address. The logs from the various nodes in your deployment specific to that particular endpoint get collected in a single file thus helping you troubleshoot your issue quickly and efficiently. You can run this troubleshooting tool only for one endpoint at a time. The log files are listed in the GUI. You can download the logs for an endpoint from a single node or from all the nodes in your deployment.

### Download Debug Logs for a Specific Endpoint

To troubleshoot issues related to a specific endpoint in your network, you can use the Debug Endpoint tool from the Admin portal. Alternatively, you can run this tool from the Authentications page. Right-click the Endpoint ID from the Authentications page and click **Endpoint Debug**. This tool provides all debug information for all services related to the specific endpoint in a single file.

**Before you begin**

You need the IP address or MAC address of the endpoint whose debug logs you want to collect.

**Step 1**  Choose **Operations > Troubleshoot > Diagnostic Tools > General Tools > Endpoint Debug**.

**Step 2**  Click the **MAC Address** or **IP** radio button and enter the MAC or IP address of the endpoint.

**Step 3**  Check the **Automatic disable after n Minutes** check box if you want to stop log collection after a specified amount of time. If you check this check box, you must enter a time between 1 and 60 minutes.

The following message appears: "Endpoint Debug degrades the deployment performance. Would you like to continue?"

**Step 4**  Click **Continue** to collect the logs.

**Step 5**  Click **Stop** when you want to manually stop the log collection.

**Related Topics**

- **Cisco ISE Debug Logs**, on page 898
- **Endpoint Debug Log Collector**, on page 275
Collection Filters

You can configure the Collection Filters to suppress the syslog messages being sent to the monitoring and external servers. The suppression can be performed at the Policy Services Node levels based on different attribute types. You can define multiple filters with specific attribute type and a corresponding value.

Before sending the syslog messages to monitoring node or external server, Cisco ISE compares these values with fields in syslog messages to be sent. If any match is found, then the corresponding message is not sent.

Configure Collection Filters

You can configure multiple collection filters based on various attribute types. It is recommended to limit the number of filters to 20. You can add, edit, or delete a collection filter.

**Step 1**  
Choose Administration > System > Logging > Collection Filters.

**Step 2**  
Click Add.

**Step 3**  
Choose the Filter Type from the following list:
- User Name
- MAC Address
- Policy Set Name
- NAS IP Address
- Device IP Address

**Step 4**  
Enter the corresponding Value for the filter type you have selected.

**Step 5**  
Choose the Result from the drop-down list. The result can be All, Passed, or Failed.

**Step 6**  
Click Submit.

Related Topics

Collection Filters, on page 276  
Event Suppression Bypass Filter, on page 276

Event Suppression Bypass Filter

Cisco ISE allows you to set filters to suppress some syslog messages from being sent to the Monitoring node and other external servers using the Collection Filters. At times, you need access to these suppressed log messages. Cisco ISE now provides you an option to bypass the event suppression based on a particular attribute such as username for a configurable amount of time. The default is 50 minutes, but you can configure the duration from 5 minutes to 480 minutes (8 hours). After you configure the event suppression bypass, it takes effect immediately. If the duration that you have set elapses, then the bypass suppression filter expires.

You can configure a suppression bypass filter from the Collection Filters page in the Cisco ISE user interface. Using this feature, you can now view all the logs for a particular identity (user) and troubleshoot issues for that identity in real time.
You can enable or disable a filter. If the duration that you have configured in a bypass event filter elapses, the filter is disabled automatically until you enable it again.

Cisco ISE captures these configuration changes in the Change Configuration Audit Report. This report provides information on who configured an event suppression or a bypass suppression and the duration of time for which the event was suppressed or the suppression bypassed.
Event Suppression Bypass Filter
CHAPTER 13

Backup and Restore Operations

• Backup Data Type, on page 279
• Backup and Restore Repositories, on page 280
• On-Demand and Scheduled Backups, on page 282
• Cisco ISE Restore Operation, on page 287
• Export Authentication and Authorization Policy Configuration, on page 293
• Synchronize Primary and Secondary Nodes in a Distributed Environment, on page 294
• Recovery of Lost Nodes in Standalone and Distributed Deployments, on page 294

Backup Data Type

Cisco ISE allows you to back up data from the Primary PAN and from the Monitoring node. Back up can be done from the CLI or user interface.

Cisco ISE allows you to back up the following type of data:

• Configuration data—Contains both application-specific and Cisco ADE operating system configuration data. Back up can be done via the Primary PAN using the GUI or CLI.

• Operational Data—Contains monitoring and troubleshooting data. Back up can be done via the Primary PAN GUI or using the CLI for the Monitoring node.

When Cisco ISE is run on VMware, VMware snapshots are not supported for backing up ISE data.

Note

Cisco ISE does not support VMware snapshots for backing up ISE data because a VMware snapshot saves the status of a VM at a given point in time. In a multi-node Cisco ISE deployment, data in all the nodes are continuously synchronized with current database information. Restoring a snapshot might cause database replication and synchronization issues. Cisco recommends that you use the backup functionality included in Cisco ISE for archival and restoration of data.

Using VMware snapshots or any third-party backup to back up ISE data results in stopping Cisco ISE services. When a backup is initiated by VMware or any third party like Comvault SAN level backup, it quiesces the file system to maintain crash consistency, which causes ISE to freeze. A reboot is required to resume the services on ISE.

Example: VM snapshots, Comvault SAN level backup, etc.
Restore operation, can be performed with the backup files of previous versions of Cisco ISE and restored on a later version. For example, if you have a backup from an ISE node from Cisco ISE, Release 1.3 or 1.4, you can restore it on Cisco ISE, Release 2.1.

Cisco ISE, Release 2.3 supports restore from backups obtained from Release 2.0 and later.

### Backup and Restore Repositories

Cisco ISE allows you to create and delete repositories through the Admin portal. You can create the following types of repositories:

- DISK
- FTP
- SFTP
- NFS
- CD-ROM
- HTTP
- HTTPS

**Note**

Repositories are local to each device.

We recommend that you have a repository size of 10 GB for small deployments (100 endpoints or less), 100 GB for medium deployments, and 200 GB for large deployments.

**Related Topics**

- [Create Repositories](#), on page 280
- [On-Demand and Scheduled Backups](#), on page 282

### Create Repositories

You can use the CLI and GUI to create repositories. We recommend that you use the GUI due to the following reasons:

- Repositories that are created through the CLI are saved locally and do not get replicated to the other deployment nodes. These repositories do not get listed in the GUI's repository page.

- Repositories that are created on the Primary PAN get replicated to the other deployment nodes.

The keys are generated only at the Primary PAN on GUI, and so during upgrade you need to generate the keys again at GUI of new primary admin and export it to the SFTP server. If you take the nodes out of the deployment, you need to generate the keys on GUI of non-admin nodes and export it to the SFTP server.

You can configure an SFTP repository in Cisco ISE with RSA public key authentication. Instead of using an administrator-created password to encrypt the database and logs, you can choose the RSA public key authentication that uses secure keys. In case of SFTP repository created with RSA public key, the repositories created through the GUI do not get replicated in the CLI and the repositories created through the CLI do not
get replicated in the GUI. To configure same repository on the CLI and GUI, generate RSA public keys on both CLI and GUI and export both the keys to the SFTP server.

Before you begin

- To perform the following task, you must be a Super Admin or System Admin.
- If you want to create an SFTP repository with RSA public key authentication, ensure that you:
  - Enable RSA public key authentication in the SFTP repository.
  - Enter the host key of the SFTP server from the Cisco ISE CLI using the `crypto host_key add` command. The host key string should match the hostname that you enter in the Path field of the repository configuration page.
  - Generate the key pairs and export the public key to your local system from the GUI. From the Cisco ISE CLI, generate the key pairs using the `crypto key generate rsa passphrase test123` command, where, passphrase must be greater than four letters, and export the keys to any repository (local disk or any other configured repository).
  - Copy the exported RSA public key to the PKI-enabled SFTP server and add it to the "authorized_keys" file.

Step 1
Choose Administration > System > Maintenance > Repository.

Step 2
Click Add to add a new repository.

Step 3
Enter the values as required to set up new repository. See Repository Settings, on page 944 for a description of the fields.

Step 4
Click Submit to create the repository.

Step 5
Verify that the repository is created successfully by clicking Repository in the Operations navigation pane on the left or click the Repository List link at the top of this page to go to the repository listing page.

What to do next

- Ensure that the repository that you have created is valid. You can do so from the Repository listing page. Select the repository and click Validate. Alternatively, you can execute the following command from the Cisco ISE command-line interface:

  ```
  show repository repository_name
  ```

  where `repository_name` is the name of the repository that you have created.

  **Note**
  If the path that you provided while creating the repository does not exist, then you will get the following error: %Invalid Directory.

- Run an on-demand backup or schedule a backup.

Related Topics

- Perform an On-Demand Backup, on page 283
- Schedule a Backup, on page 284
Enable RSA Public Key Authentication in SFTP Repository

To enable RSA public key authentication in SFTP repository:

**Step 1** Log in to SFTP server with an account that has permission to edit the `/etc/ssh/sshd_config` file.

*Note* The location of the `sshd_config` file might vary based on the operating system installation.

**Step 2** Enter the `vi /etc/ssh/sshd_config` command.

The contents of the `sshd_config` file is listed.

**Step 3** Remove the "#" symbol from the following lines to enable RSA public key authentication:

- RSAAuthentication yes
- PubkeyAuthentication yes

*Note* If Public Auth Key is no, change it to yes.

- AuthorizedKeysFile `~/.ssh/authorized_keys`

---

**On-Demand and Scheduled Backups**

Cisco ISE provides on-demand backups of the Primary PAN and the primary monitoring node. Perform an on-demand backup when you want to backup data immediately.

Cisco ISE also allows you to schedule system-level backups that can be scheduled to run once, daily, weekly, or monthly. Because backup operations can be lengthy, you can schedule them so they are not a disruption. You can schedule a backup from the Cisco ISE Admin portal.

*Note* If you upgrade to Cisco ISE, Release 1.2, the scheduled backup jobs need to be recreated.

**Related Topics**

- Schedule a Backup, on page 284
- Perform an On-Demand Backup, on page 283
- Backup Using the CLI, on page 286
- Backup History, on page 286
- Backup Failures, on page 286
- Cisco ISE Restore Operation, on page 287
- Maintenance Settings, on page 944
Perform an On-Demand Backup

You can perform an On-demand backup to instantly backup the configuration or monitoring (operational) data. The restore operation restores Cisco ISE to the configuration state that existed at the time of obtaining the backup.

---

Important

When performing a backup and restore, the restore overwrites the list of trusted certificates on the target system with the list of certificates from the source system. It is critically important to note that backup and restore functions do not include private keys associated with the Internal Certificate Authority (CA) certificates.

If you are performing a backup and restore from one system to another, you will have to choose from one of these options to avoid errors:

- **Option 1:**
  
  Export the CA certificates from the source ISE node through the CLI and import them in to the target system through the CLI.
  
  **Pros:** Any certificates issued to endpoints from the source system will continue to be trusted. Any new certificates issued by the target system will be signed by the same keys.
  
  **Cons:** Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

- **Option 2:**
  
  After the restore process, generate all new certificates for the internal CA.
  
  **Pros:** This option is the recommended and clean method, where neither the original source certificates or the original target certificates will be used. Certificates issued by the original source system will continue to be trusted.
  
  **Cons:** Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

---

Before you begin

- Before you perform this task, you should have a basic understanding of the backup data types in Cisco ISE.
- Ensure that you have created repositories for storing the backup file.
- Do not back up using a local repository. You cannot back up the monitoring data in the local repository of a remote Monitoring node.
- Ensure that you perform all certificate-related changes before you obtain the backup.
- To perform the following task, you must be a Super Admin or System Admin.

---

Note

For backup and restore operations, the following repository types are not supported: CD-ROM, HTTP, HTTPS, or TFTP. This is because, either these repository types are read-only or the protocol does not support file listing. To restore a backup, choose the repository and click **Restore.**
Step 1 Choose Administration > System > Backup and Restore.
Step 2 Choose the type of backup: Configuration or Operational.
Step 3 Click Backup Now.
Step 4 Enter the values as required to perform a backup.
Step 5 Click Backup.
Step 6 Verify that the backup completed successfully.

Cisco ISE appends the backup filename with a timestamp and stores the file in the specified repository. In addition to the timestamp, Cisco ISE adds a CFG tag for configuration backups and OPS tag for operational backups. Ensure that the backup file exists in the specified repository.

In a distributed deployment, do not change the role of a node or promote a node when the backup is running. Changing node roles will shut down all the processes and might cause some inconsistency in data if a backup is running concurrently. Wait for the backup to complete before you make any node role changes.

Do not promote a node when the backup is running. This will shut down all the processes and might cause some inconsistency in data if a backup is running concurrently. Wait for the backup to complete before you make any node changes.

Note: High CPU usage might be observed and High Load Average alarm might be seen when the backup is running. CPU usage will be back to normal when the backup is complete.

Related Topics
- Backup Data Type, on page 279
- Create Repositories, on page 280
- Backup and Restore Repositories, on page 280
- Schedule a Backup, on page 284
- Backup Using the CLI, on page 286
- Backup History, on page 286
- Backup Failures, on page 286
- Cisco ISE Restore Operation, on page 287
- Export Authentication and Authorization Policy Configuration, on page 293

Schedule a Backup

You can perform an On-demand backup to instantly backup the configuration or monitoring (operational) data. The restore operation restores Cisco ISE to the configuration state that existed at the time of obtaining the backup.
When performing a backup and restore, the restore overwrites the list of trusted certificates on the target system with the list of certificates from the source system. It is critically important to note that backup and restore functions do not include private keys associated with the Internal Certificate Authority (CA) certificates.

If you are performing a backup and restore from one system to another, you will have to choose from one of these options to avoid errors:

- **Option 1:**
  Export the CA certificates from the source ISE node through the CLI and import them in to the target system through the CLI.
  **Pros:** Any certificates issued to endpoints from the source system will continue to be trusted. Any new certificates issued by the target system will be signed by the same keys.
  **Cons:** Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

- **Option 2:**
  After the restore process, generate all new certificates for the internal CA.
  **Pros:** This option is the recommended and clean method, where neither the original source certificates or the original target certificates will be used. Certificates issued by the original source system will continue to be trusted.
  **Cons:** Any certificates that have been issued by the target system prior to the restore function will not be trusted and will need to be re-issued.

---

**Before you begin**

- Before you perform this task, you should have a basic understanding of the backup data types in Cisco ISE.
- Ensure that you have configured repositories.
- Do not back up using a local repository. You cannot back up the monitoring data in the local repository of a remote Monitoring node.
- To perform the following task, you must be a Super Admin or System Admin.
- If you have upgraded to Cisco ISE 1.2 from Cisco ISE 1.1 or earlier releases, you should reconfigure your scheduled backups. See the Known Upgrade Issues section in the *Cisco Identity Services Engine Upgrade Guide, Release 1.2*.

**Note**

For backup and restore operations, the following repository types are not supported: CD-ROM, HTTP, HTTPS, or TFTP. This is because, either these repository types are read-only or the protocol does not support file listing.

---

**Step 1**  Choose Administration > System > Backup and Restore.
Step 2  Click **Schedule** to schedule a Configuration or an Operational backup.

Step 3  Enter the values as required to schedule a backup.

Step 4  Click **Save** to schedule the backup.

Step 5  Perform one of the following actions:

- From the **Select Repository** drop-down list, choose the required repository.
- Click the **Add Repository** link to add a new repository.

Step 6  Click the **Refresh** link to see the scheduled backup list.

You can create only one schedule at a time for a Configuration or Operational backup. You can enable or disable a scheduled backup, but you cannot delete it.

---

**Related Topics**

- [Backup Data Type](#), on page 279
- [On-Demand and Scheduled Backups](#), on page 282
- [Perform an On-Demand Backup](#), on page 283
- [Backup Using the CLI](#), on page 286
- [Backup History](#), on page 286
- [Backup Failures](#), on page 286
- [Backup and Restore Repositories](#), on page 280

---

**Backup Using the CLI**

Although you can schedule backups both from the CLI as well as the GUI, it is recommended to use GUI for better options. But, you can perform Operational backup on the secondary monitoring node only from the CLI.

**Backup History**

Backup history provides basic information about scheduled and on-demand backups. It lists the name of the backup, backup file size, repository where the backup is stored, and time stamp that indicates when the backup was obtained. This information is available in the Operations Audit report and on the Backup and Restore page in the History table.

For failed backups, Cisco ISE triggers an alarm. The backup history page provides the failure reason. The failure reason is also cited in the Operations Audit report. If the failure reason is missing or is not clear, you can run the **backup-logs** command from the Cisco ISE CLI and look at the ADE.log for more information.

While the backup operation is in progress, you can use the **show backup status** CLI command to check the progress of the backup operation.

Backup history is stored along with the Cisco ADE operating system configuration data. It remains there even after an application upgrade and are only removed when you reimage the PAN.

**Backup Failures**

If backup fails, check the following:
• Make sure that no other backup is running at the same time.

• Check the available disk space for the configured repository.
  • Monitoring (operational) backup fails if the monitoring data takes up more than 75% of the allocated monitoring database size. For example, if your Monitoring node is allocated 600 GB, and the monitoring data takes up more than 450 GB of storage, then monitoring backup fails.
  • If the database disk usage is greater than 90%, a purge occurs to bring the database size to less than or equal to 75% of its allocated size.

• Verify if a purge is in progress. Backup and restore operations will not work while a purge is in progress.

• Verify if the repository is configured correctly.

Cisco ISE Restore Operation

You can restore configuration data on a primary or standalone administration node. After you restore data on the Primary PAN, you must manually synchronize the secondary nodes with the Primary PAN.

The process for restoring the operational data is different depending on the type of deployment.

Note

The new backup/restore user interface in Cisco ISE makes use of meta-data in the backup filename. Therefore, after a backup completes, you should not modify the backup filename manually. If you manually modify the backup filename, the Cisco ISE backup/restore user interface will not be able to recognize the backup file. If you have to modify the backup filename, you should use the Cisco ISE CLI to restore the backup.

Related Topics

  Restoration of Configuration or Monitoring (Operational) Backup from the CLI, on page 288
  Restore Configuration Backups from the GUI, on page 290
  Restoration of Monitoring Database, on page 291
  Synchronize Primary and Secondary Nodes in a Distributed Environment, on page 294

Guidelines for Data Restoration

Following are guidelines to follow when you restore Cisco ISE backup data.

• Cisco ISE allows you to obtain a backup from an ISE node (A) and restore it on another ISE node (B), both having the same host names (but different IP addresses). However, after you restore the backup on node B, do not change the hostname of node B because it might cause issues with certificates and portal group tags.

• If you obtain a backup from the Primary PAN in one timezone and try to restore it on another Cisco ISE node in another timezone, the restore process might fail. This failure happens if the timestamp in the backup file is later than the system time on the Cisco ISE node on which the backup is restored. If you restore the same backup a day after it was obtained, then the timestamp in the backup file is in the past and the restore process succeeds.
• When you restore a backup on the Primary PAN with a different hostname than the one from which the backup was obtained, the Primary PAN becomes a standalone node. The deployment is broken and the secondary nodes become nonfunctional. You must make the standalone node the primary node, reset the configuration on the secondary nodes, and reregister them with the primary node. To reset the configuration on Cisco ISE nodes, enter the following command from the Cisco ISE CLI:

  • application reset-config ise

• We recommend that you do not change the system timezone after the initial Cisco ISE installation and setup.

• If you changed the certificate configuration on one or more nodes in your deployment, you must obtain another backup to restore the data from the standalone Cisco ISE node or Primary PAN. Otherwise, if you try to restore data using an older backup, the communication between the nodes might fail.

• After you restore the configuration backup on the Primary PAN, you can import the Cisco ISE CA certificates and keys that you exported earlier.

  Note  
  If you did not export the Cisco ISE CA certificates and keys, then after you restore the configuration backup on the Primary PAN, generate the root CA and subordinate CAs on the Primary PAN and Policy Service Nodes (PSNs).

• If you are trying to restore a platinum database without using the correct FQDN (FQDN of a platinum database), you need to regenerate the CA certificates. (choose Administration > Certificates > Certificate Signing Requests > Replace ISE Root CA certificate chain). However, If you restore the platinum database with the correct FQDN, note that the CA certificates regenerated automatically.

• You need a data repository, which is the location where Cisco ISE saves your backup file. You must create a repository before you can run an on-demand or scheduled backup.

• If you have a standalone administration node that fails, you must run the configuration backup to restore it. If the Primary PAN fails, you can use the distributed setup to promote your Secondary Administration Node to become the primary. You can then restore data on the Primary PAN after it comes up.

  Note  
  Cisco ISE also provides the backup-logs CLI command that you can use to collect log and configuration files for troubleshooting purposes.

## Restoration of Configuration or Monitoring (Operational) Backup from the CLI

To restore configuration data through the Cisco ISE CLI, use the restore command in the EXEC mode. Use the following command to restore data from a configuration or operational backup:

```
restore filename repository repository-name encryption-key hash|plain encryption-key name include-adeos
```

### Syntax Description

| restore | Type this command to restore data from a configuration or operational backup. |
Restoration of Configuration or Monitoring (Operational) Backup from the CLI

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filename</td>
<td>Name of the backed-up file that resides in the repository. Supports up to 120 alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> You must add the .tar.gpg extension after the filename (for example, myfile.tar.gpg).</td>
</tr>
<tr>
<td>repository</td>
<td>Specifies the repository that contains the backup.</td>
</tr>
<tr>
<td>repository-name</td>
<td>Name of the repository you want to restore the backup from.</td>
</tr>
<tr>
<td>encryption-key</td>
<td>(Optional) Specifies user-defined encryption key to restore backup.</td>
</tr>
<tr>
<td>hash</td>
<td>Hashed encryption key for restoring backup. Specifies an encrypted (hashed) encryption key that follows. Supports up to 40 characters.</td>
</tr>
<tr>
<td>plain</td>
<td>Plaintext encryption key for restoring backup. Specifies an unencrypted plaintext encryption key that follows. Supports up to 15 characters.</td>
</tr>
<tr>
<td>encryption-key name</td>
<td>Enter the encryption key.</td>
</tr>
<tr>
<td>include-adeos</td>
<td>(Optional, applicable only for configuration backup) Enter this command operator parameter if you want to restore ADE-OS configuration from a configuration backup. When you restore a configuration backup, if you do not include this parameter, Cisco ISE restores only the Cisco ISE application configuration data.</td>
</tr>
</tbody>
</table>

**Defaults**

No default behavior or values.

**Command Modes**

EXEC

**Usage Guidelines**

When you use restore commands in Cisco ISE, the Cisco ISE server restarts automatically.

The encryption key is optional while restoring data. To support restoring earlier backups where you have not provided encryption keys, you can use the **restore** command without the encryption key.

**Examples**

```
ise/admin# restore mybackup-100818-1502.tar.gpg repository myrepository encryption-key plain Lab12345
```

Restore may require a restart of application services. Continue? (yes/no) [yes] ? yes
Initiating restore. Please wait...
ISE application restore is in progress.
This process could take several minutes. Please wait...
Stopping ISE Application Server...
Stopping ISE Monitoring & Troubleshooting Log Processor...
Stopping ISE Monitoring & Troubleshooting Log Collector...
Stopping ISE Monitoring & Troubleshooting Session Database...
Stopping ISE Database processes...
Starting ISE Database processes...
Starting ISE Monitoring & Troubleshooting Session Database...
Starting ISE Application Server...
Starting ISE Monitoring & Troubleshooting Alert Process...
Starting ISE Monitoring & Troubleshooting Log Collector...
Starting ISE Monitoring & Troubleshooting Log Processor...
Note: ISE Processes are initializing. Use 'show application status ise' CLI to verify all processes are in running state.

ise/admin#

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>backup</td>
<td>Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.</td>
</tr>
<tr>
<td>backup-logs</td>
<td>Backs up system logs.</td>
</tr>
<tr>
<td>repository</td>
<td>Enters the repository submode for configuration of backups.</td>
</tr>
<tr>
<td>show repository</td>
<td>Displays the available backup files located on a specific repository.</td>
</tr>
<tr>
<td>show backup history</td>
<td>Displays the backup history of the system.</td>
</tr>
<tr>
<td>show backup status</td>
<td>Displays the status of the backup operation.</td>
</tr>
<tr>
<td>show restore status</td>
<td>Displays the status of the restore operation.</td>
</tr>
</tbody>
</table>

If the sync status and replication status after application restore for any secondary node is *Out of Sync*, you have to reimport the certificate of that secondary node to the Primary PAN and perform a manual synchronization.

**Related Topics**

- [Restore Configuration Backups from the GUI](#), on page 290
- [Restore History](#), on page 293
- [Synchronize Primary and Secondary Nodes in a Distributed Environment](#), on page 294

### Restore Configuration Backups from the GUI

You can restore a configuration backup from the Admin portal. The GUI lists only the backups that are taken from the current release. To restore backups that are prior to this release, use the restore command from the CLI.
Before you begin

Ensure that the Primary PAN auto-failover configuration, if enabled in your deployment, is turned off. When you restore a configuration backup, the application server processes are restarted. There might be a delay while these services restart. Due to this delay in restart of services, auto-failover of Secondary PAN might get initiated.

Step 1
Choose Administration > System > Backup and Restore.

Step 2
Select the name of the backup from the list of Configurational backup and click Restore.

Step 3
Enter the Encryption Key used during the backup.

Step 4
Click Restore.

What to do next

If you are using the Cisco ISE CA service, you must:

1. Regenerate the entire Cisco ISE CA root chain.

2. Obtain a backup of the Cisco ISE CA certificates and keys from the Primary PAN and restore it on the Secondary PAN. This ensures that the Secondary PAN can function as the root CA or subordinate CA of an external PKI in case of a Primary PAN failure and you promote the Secondary PAN to be the Primary PAN.

Related Topics

- Restoration of Configuration or Monitoring (Operational) Backup from the CLI, on page 288

Restoration of Monitoring Database

The process for restoring the Monitoring database is different depending on the type of deployment. The following sections explain how to restore the Monitoring database in standalone and distributed deployments.

You must use the CLI to restore an on-demand Monitoring database backup from previous releases of Cisco ISE. Restoring a scheduled backup across Cisco ISE releases is not supported.

Note

If you attempt to restore data to a node other than the one from which the data was taken, you must configure the logging target settings to point to the new node. This ensures that the monitoring syslogs are sent to the correct node.

Related Topics

- Restore a Monitoring (Operational) Backup in a Standalone Environment, on page 291
- Restore a Monitoring Backup with Administration and Monitor Personas, on page 292
- Restore a Monitoring Backup with a Monitoring Persona, on page 293

Restore a Monitoring (Operational) Backup in a Standalone Environment

The GUI lists only the backups that are taken from the current release. To restore backups that obtained from earlier releases, use the restore command from the CLI.
Before you begin

- Purge the old monitoring data.
- Schedule a backup or perform an on-demand backup.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; System &gt; Backup and Restore.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select the name of the backup from the list of Operational backup and click Restore.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the Encryption Key used during the backup.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Restore.</td>
</tr>
</tbody>
</table>

Related Topics

Schedule a Backup, on page 284
Perform an On-Demand Backup, on page 283
Restoration of Configuration or Monitoring (Operational) Backup from the CLI, on page 288
Restore a Monitoring Backup with Administration and Monitor Personas, on page 292
Restore a Monitoring Backup with a Monitoring Persona, on page 293

Restore a Monitoring Backup with Administration and Monitor Personas

You can restore a Monitoring backup in a distributed environment with Administration and Monitor personas.

Before you begin

- Purge the old monitoring data.
- Schedule a backup or perform an on-demand backup.

| Step 1 | If you are using a primary and secondary PAN, synchronize the PANs.  
When you synchronize the PANs, you must chose a PAN an promote that to be the active primary. |
|--------|--------------------------------------------------------------------------------------------------|
| Step 2 | Before you deregister the Monitoring node, assign the Monitoring persona to another node in the deployment.  
Every deployment must have at least one functioning Monitoring node. |
| Step 3 | Deregister the Monitoring node to be backed up. |
| Step 4 | Restore the Monitoring backup to the newly deregistered node. |
| Step 5 | Register the newly restored node with the current Administration node. |
| Step 6 | Promote the newly restored and registered node as the active Monitoring node. |

Related Topics

Schedule a Backup, on page 284
Perform an On-Demand Backup, on page 283
Synchronize Primary and Secondary Nodes in a Distributed Environment, on page 294
Restore a Monitoring (Operational) Backup in a Standalone Environment, on page 291
Restore a Monitoring Backup with a Monitoring Persona, on page 293
Restore a Monitoring Backup with a Monitoring Persona

You can restore a Monitoring backup in a distributed environment with only Monitoring persona.

**Before you begin**
- Purge the old monitoring data.
- Schedule a backup or perform an on-demand backup.

---

**Step 1**
Prepare to deregister the node to be restored by assigning the Monitoring persona to another node in the deployment. A deployment must have at least one functioning Monitoring node.

**Step 2**
Deregister the node to be restored.

*Note* Wait until the deregistration is complete before proceeding with the restore. The node must be in a standalone state before you can continue with the restore.

**Step 3**
Restore the Monitoring backup to the newly deregistered node.

**Step 4**
Register the newly restored node with the current Administration node.

**Step 5**
Promote the newly restored and registered node as the PAN.

---

**Related Topics**
- Restore a Monitoring (Operational) Backup in a Standalone Environment, on page 291
- Restore a Monitoring Backup with Administration and Monitor Personas, on page 292

---

**Restore History**

You can obtain information about all restore operations, log events, and statuses from the Operations Audit report.

*Note* However, the Operations Audit report does not provide information about the start times corresponding to the previous restore operations.

For troubleshooting information, you have to run the `backup-logs` command from the Cisco ISE CLI and look at the ADE.log file.

While the restore operation is in progress, all Cisco ISE services are stopped. You can use the `show restore status` CLI command to check the progress of the restore operation.

---

**Export Authentication and Authorization Policy Configuration**

You can export authentication and authorization policy configuration in the form of an XML file that you can read offline to identify any configuration errors and use for troubleshooting purposes. This XML file includes authentication and authorization policy rules, simple and compound policy conditions, dACLs, and authorization profiles. You can choose to email the XML file or save it to your local system.
**Synchronize Primary and Secondary Nodes in a Distributed Environment**

In a distributed environment, sometimes the Cisco ISE database in the primary and secondary nodes are not synchronized automatically after restoring a backup file on the PAN. If this happens, you can manually force a full replication from the PAN to the secondary ISE nodes. You can force a synchronization only from the PAN to the secondary nodes. During the sync-up operation, you cannot make any configuration changes. Cisco ISE allows you to navigate to other Cisco ISE Admin portal pages and make any configuration changes only after the synchronization is complete.

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

### Step 1
Choose **Administration > System > Deployment**.

### Step 2
Check the checkboxes next to the secondary ISE nodes with an Out of Sync replication status.

### Step 3
Click **Syncup** and wait until the nodes are synchronized with the PAN. You will have to wait until this process is complete before you can access the Cisco ISE Admin portal again.

**Recovery of Lost Nodes in Standalone and Distributed Deployments**

This section provides troubleshooting information that you can use to recover lost nodes in standalone and distributed deployments. Some of the following use cases use the backup and restore functionality and others use the replication feature to recover lost data.
Recovery of Lost Nodes Using Existing IP Addresses and Hostnames in a Distributed Deployment

Scenario

In a distributed deployment, a natural disaster leads to a loss of all the nodes. After recovery, you want to use the existing IP addresses and hostnames.

For example, you have two nodes: N1 (Primary Policy Administration Node or Primary PAN) and N2 (Secondary Policy Administration Node or Secondary PAN.) A backup of the N1 node, which was taken at time T1, is available. Later, both N1 and N2 nodes fail because of a natural disaster.

Assumption

All Cisco ISE nodes in the deployment were destroyed. The new hardware was imaged using the same hostnames and IP addresses.

Resolution Steps

1. You have to replace both the N1 and N2 nodes. N1 and N2 nodes will now have a standalone configuration.
2. Obtain a license with the UDI of the N1 and N2 nodes and install it on the N1 node.
3. You must then restore the backup on the replaced N1 node. The restore script will try to sync the data on N2, but N2 is now a standalone node and the synchronization fails. Data on N1 will be reset to time T1.
4. You must log in to the N1 Admin portal to delete and reregister the N2 node. Both the N1 and N2 nodes will have data reset to time T1.

Related Topics

Restoration of Configuration or Monitoring (Operational) Backup from the CLI, on page 288

Recovery of Lost Nodes Using New IP Addresses and Hostnames in a Distributed Deployment

Scenario

In a distributed deployment, a natural disaster leads to loss of all the nodes. The new hardware is reimaged at a new location and requires new IP addresses and hostnames.

For example, you have two ISE nodes: N1 (Primary Policy Administration Node or Primary PAN) and N2 (Secondary Policy Service Node.) A backup of the N1 node which was taken at time T1, is available. Later, both N1 and N2 nodes fail because of a natural disaster. The Cisco ISE nodes are replaced at a new location and the new hostnames are N1A (Primary PAN) and N2A (Secondary Policy Service Node). N1A and N2A are standalone nodes at this point in time.

Assumptions

All Cisco ISE nodes in the deployment were destroyed. The new hardware was imaged at a different location using different hostnames and IP addresses.
Resolution Steps

1. Obtain the N1 backup and restore it on N1A. The restore script will identify the hostname change and domain name change, and will update the hostname and domain name in the deployment configuration based on the current hostname.

2. You must generate a new self-signed certificate.

3. You must log in to the Cisco ISE Admin portal on N1A, choose Administration > System > Deployment, and do the following:
   - Delete the old N2 node.
   - Register the new N2A node as a secondary node. Data from the N1A node will be replicated to the N2A node.

Related Topics
   - Restoration of Configuration or Monitoring (Operational) Backup from the CLI, on page 288

Recovery of a Node Using Existing IP Address and Hostname in a Standalone Deployment

Scenario

A standalone administration node is down.

For example, you have a standalone administration node, N1. A backup of the N1 database was taken at time T1. The N1 node goes down because of a physical failure and must be reimaged or a new hardware is required. The N1 node must be brought back up with the same IP address and hostname.

Assumptions

This deployment is a standalone deployment and the new or reimaged hardware has the same IP address and hostname.

Resolution Steps

Once the N1 node is up after a reimage or you have introduced a new Cisco ISE node with the same IP address and hostname, you must restore the backup taken from the old N1 node. You do not have to make any role changes.

Related Topics
   - Restoration of Configuration or Monitoring (Operational) Backup from the CLI, on page 288

Recovery of a Node Using New IP Address and Hostname in a Standalone Deployment

Scenario

A standalone administration node is down.
For example, you have a standalone administration node, N1. A backup of the N1 database taken at time T1 is available. The N1 node is down because of a physical failure and will be replaced by a new hardware at a different location with a different IP address and hostname.

**Assumptions**

This is a standalone deployment and the replaced hardware has a different IP address and hostname.

**Resolution Steps**

1. Replace the N1 node with a new hardware. This node will be in a standalone state and the hostname is N1B.
2. You can restore the backup on the N1B node. No role changes are required.

**Related Topics**

Restoration of Configuration or Monitoring (Operational) Backup from the CLI, on page 288

---

**Configuration Rollback**

**Problem**

There may be instances where you inadvertently make configuration changes that you later determine were incorrect. For example, you may delete several NADs or modify some RADIUS attributes incorrectly and realize this issue several hours later. In this case, you can revert back to the original configuration by restoring a backup that was taken before you made the changes.

**Possible Causes**

There are two nodes: N1 (Primary Policy Administration Node or Primary PAN) and N2 (Secondary Policy Administration Node or Secondary PAN) and a backup of the N1 node is available. You made some incorrect configuration changes on N1 and want to remove the changes.

**Solution**

Obtain a backup of the N1 node that was taken before the incorrect configuration changes were made. Restore this backup on the N1 node. The restore script will synchronize the data from N1 to N2.

**Related Topics**

Restoration of Configuration or Monitoring (Operational) Backup from the CLI, on page 288

---

**Recovery of Primary Node in Case of Failure in a Distributed Deployment**

**Scenario**

In a multinode deployment, the PAN fails.

For example, you have two Cisco ISE nodes, N1 (PAN) and N2 (Secondary Administration Node). N1 fails because of hardware issues.
Assumptions

Only the primary node in a distributed deployment has failed.

Resolution Steps

1. Log in to the N2 Admin portal. Choose Administration > System > Deployment and configure N2 as your primary node.

   The N1 node is replaced with a new hardware, reimaged, and is in the standalone state.

2. From the N2 Admin portal, register the new N1 node as a secondary node.

   Now, the N2 node becomes your primary node and the N1 node becomes your secondary node.

If you wish to make the N1 node the primary node again, log in to the N1 Admin portal and make it the primary node. N2 automatically becomes a secondary server. There is no data loss.

Recovery of Secondary Node in Case of Failure in a Distributed Deployment

Scenario

In a multinode deployment, a single secondary node has failed. No restore is required.

For example, you have multiple nodes: N1 (Primary PAN), N2 (Secondary PAN), N3 (Secondary Policy Service Node), N4 (Secondary Policy Service Node). One of the secondary nodes, N3, fails.

Resolution Steps

1. Reimage the new N3A node to the default standalone state.

2. Log in to the N1 Admin portal and delete the N3 node.

3. Reregister the N3A node.

   Data is replicated from N1 to N3A. No restore is required.
Setup Adaptive Network Control

- Enable Adaptive Network Control in Cisco ISE, on page 299
- Configure Network Access Settings, on page 299
- Adaptive Network Control, on page 301
- ANC Quarantine and Unquarantine Flow, on page 303
- ANC NAS Port Shutdown Flow, on page 303
- Endpoints Purge Settings, on page 304

Enable Adaptive Network Control in Cisco ISE

Adaptive Network Control (ANC) is disabled by default. It gets enabled only when pxGrid is enabled and it remains enabled until you manually disable the service in the Admin portal.

Related Topics
- Configure Network Access Settings, on page 299

Configure Network Access Settings

Adaptive Network Control (ANC) allows you to reset the network access status of an endpoint to quarantine, unquarantine, or shutdown a port, which defines authorization to the network depending on the network access status.

You can quarantine or unquarantine endpoints, or shut down the network access server (NAS) ports to which endpoints are connected, by using their endpoint IP addresses or MAC addresses. You can perform quarantine and unquarantine operations on the same endpoint multiple times, provided they are not performed simultaneously. If you discover a hostile endpoint on your network, you can shut down the endpoint’s access, using ANC to close the NAS port.

To assign an ANC policy to an endpoint:

Before you begin
- You must enable ANC.
- You must create authorization profiles and Exception type authorization policies for ANC.
**Step 1** Choose **Operations > Adaptive Network Control > Policy List.**

**Step 2** Click **Add.**

**Step 3** Enter a name for the ANC policy and specify the ANC action. The following options are available:

- Quarantine
- Shut_Down
- Port_Bounce

You can select one or multiple actions, but you cannot combine Shut_Down and Port_Bounce with the other ANC actions.

**Step 4** Choose **Policy > Policy Sets,** and expand the policy set.

**Step 5** Associate the ANC policy with the corresponding authorization policy by using the ANCPolicy attribute.

**Step 6** Choose **Operations > Adaptive Network Control > Endpoint Assignment.**

**Step 7** Click **Add.**

**Step 8** Enter the IP address or MAC address of the endpoint and select the policy from the **Policy Assignment** drop-down list.

**Step 9** Click **Submit.**

---

### Related Topics

**Quarantined Endpoints Do Not Renew Authentication Following Policy Change**, on page 300

---

### Quarantined Endpoints Do Not Renew Authentication Following Policy Change

**Problem**

Authentication has failed following a change in policy or additional identity and no reauthentication is taking place. Authentication fails or the endpoint in question remains unable to connect to the network. This issue often occurs on client machines that are failing posture assessment per the posture policy that is assigned to the user role.

**Possible Causes**

The authentication timer setting is not correctly set on the client machine, or the authentication interval is not correctly set on the switch.

**Solution**

There are several possible resolutions for this issue:

1. Check the Session Status Summary report in Cisco ISE for the specified NAD or switch, and ensure that the interface has the appropriate authentication interval configured.

2. Enter “show running configuration” on the NAD/switch and ensure that the interface is configured with an appropriate “authentication timer restart” setting. (For example, “authentication timer restart 15,” and “authentication timer reauthenticate 15.”)

3. Try entering “interface shutdown” and “no shutdown” to bounce the port on the NAD/switch and force reauthentication following a potential configuration change in Cisco ISE.
Because CoA requires a MAC address or session ID, we recommend that you do not bounce the port that is shown in the Network Device SNMP report.

Adaptive Network Control

Adaptive Network Control (ANC) is a service that runs on the Administration node that can be used for monitoring and controlling network access of endpoints. ANC can be invoked by the ISE administrator on the admin GUI and also through pxGrid from third party systems. ANC supports wired and wireless deployments and requires a Plus License.

You can use ANC to change the authorization state without having to modify the overall authorization policy of the system. ANC allows you to set the authorization state when you quarantine an endpoint as a result of established authorization policies where authorization policies are defined to check for EPSStatus to limit or deny network access. You can unquarantine an endpoint for full network access. You can also shut down the port on the network attached system (NAS) that disconnects the endpoint from the network.

There are no limits to the number of users that can be quarantined at one time, and there are no time constraints on the length of the quarantine period.

You can perform the following operations to monitor and control network access through ANC:

• Quarantine—Allows you to use Exception policies (authorization policies) to limit or deny an endpoint access to the network. You must create Exception policies to assign different authorization profiles (permissions) depending on the EPSStatus. Setting to the Quarantine state essentially moves an endpoint from its default VLAN to a specified Quarantine VLAN. You must define the Quarantine VLAN previously that is supported on the same NAS as the endpoint.

• Unquarantine—Allows you to reverse the quarantine status that permits full access to the network for an endpoint returning the endpoint to its original VLAN.

• Shutdown—Allows you to deactivate a port on the NAS and disconnect the endpoint from the network. Once the port is shutdown on the NAS to which an endpoint is connected, you must manually reset the port on the NAS again to allow an endpoint to connect to the network, which is not available for wireless deployments.

Quarantine and unquarantine operations can be triggered from the session directory reports for active endpoints.

If a quarantined session is unquarantined, the initiation method for a newly unquarantined session depends on the authentication method that is specified by the switch configuration.

Related Topics

Create Authorization Profiles for Network Access through ANC, on page 302
ANC Operations Fail when IP Address or MAC Address is not Found, on page 302
Externally Authenticated Administrators Cannot Perform ANC Operations, on page 302
Create Authorization Profiles for Network Access through ANC

You must create an authorization profile for use with ANC and the authorization profile appears in the list of Standard Authorization Profiles. An endpoint can be authenticated and authorized in the network, but restricted to access network.

Step 2 Click Add.
Step 3 Enter a unique name and description for the authorization profile, and leave the Access Type as ACCESS_ACCEPT.
Step 4 Check the DACL Name check box, and choose DENY_ALL_TRAFFIC from the drop-down list.
Step 5 Click Submit.

Exception authorization polices are intended for authorizing limited access to meet special conditions or permissions or an immediate requirement. For ANC authorization, you must create a quarantine exception policy that is processed before all standard authorization policies. You must create an exception rule with the following condition: Session·EPSSStatus EQUALS Quarantine.

ANC Operations Fail when IP Address or MAC Address is not Found

An ANC operation that you perform on an endpoint fails when an active session for that endpoint does not contain information about the IP address. This also applies to the MAC address and session ID for that endpoint.

Note When you want to change the authorization state of an endpoint through ANC, you must provide the IP address or the MAC address for the endpoint. If the IP address or the MAC address is not found in the active session for the endpoint, then you will see the following error message: No active session found for this MAC address, IPAddress or Session ID.

Externally Authenticated Administrators Cannot Perform ANC Operations

If an externally authenticated administrator tries to issue CoA-Quarantine from a live session, Cisco ISE returns the following error message:

CoA Action of Quarantine for xx:xx:xx:xx:xx:xx can not be initiated. (Cause:User not found internally. Possible use of unsupported externally authenticated user

If an externally authenticated administrator performs an ANC operation from Operations > Adaptive Network Control in the Cisco ISE Admin portal using the IP address or MAC address of the endpoint, Cisco ISE returns the following error message:

Server failure: User not found internally. Possible use of unsupported externally authenticated user
ANC Quarantine and Unquarantine Flow

You can quarantine selected endpoints with ANC, to limit their access to the network. You can quarantine endpoints and establish exception authorization policies that assign different authorization profiles, depending on the status. An authorization profile acts as a container for permissions that you define in the authorization policies that allow access to specified network services. When the authorization is complete, the permissions are granted for a network access request. If the endpoint is then validated, you can unquarantine the endpoint to allow it full access to the network.

This figure illustrates the quarantine flow, which assumes that authorization rules have been configured and the ANC session has been established.

*Figure 20: ANC Quarantine Flow*

1. A client device logs onto the network through a wireless device (WLC), and a quarantine REST API call is issued from the Administration node (PAP) to the Monitoring node (MnT).
2. The Monitoring node then calls PrRT through the Policy Services ISE node (PDP) to invoke a CoA.
3. The client device is disconnected.
4. The client device then reauthenticates and reconnects.
5. A RADIUS request for the client device is sent back to the Monitoring node.
6. The client device is quarantined while the check is made.
7. The Q-Profile authorization policy is applied, and the client device is validated.
8. The client device is unquarantined, and allowed full access to the network.

ANC NAS Port Shutdown Flow

You can shut down the NAS port to which an endpoint is connected by using the endpoint IP address or MAC address.
Shutdown allows you to close a NAS port based on a specified IP address for a MAC address, and you have to manually reinstate the port to bring the endpoint back into the network, which is effective only for endpoints that are connected through wired media.

Shutdown may not be supported on all devices. Most switches should support the shutdown command, however. You can use the getResult() command to verify that the shutdown executed successfully.

This figure illustrates the ANC shutdown flow. For the client device in the illustration, the shutdown operation is performed on the NAS that the client device uses to access the network.

**Figure 21: ANC Shutdown Flow**

---

**Endpoints Purge Settings**

You can define the Endpoint Purge Policy by configuration rules based on identity groups and other conditions using Administration > Identity Management > Settings > Endpoint Purge. You can choose not to purge specified endpoints and to purge endpoints based on selected profiling conditions.

You can schedule an endpoint purge job. This endpoint purge schedule is enabled by default. Cisco ISE, by default, deletes endpoints and registered devices that are older than 30 days. The purge job runs at 1 AM every day based on the time zone configured in the Primary PAN.

The following are some of the conditions with examples you can use for purging the endpoints:

- **InactivityDays**—Number of days since last profiling activity or update on endpoint.
  - This condition purges stale devices that have accumulated over time, commonly transient guest or personal devices, or retired devices. These endpoints tend to represent noise in most deployments as they are no longer active on network or likely to be seen in near future. If they do happen to connect again, then they will be rediscovered, profiled, registered, etc as needed.
  - When there are updates from endpoint, InactivityDays will be reset to 0 only if profiling is enabled.

- **ElapsedDays**—Numbers days since object is created.
  - This condition can be used for endpoints that have been granted unauthenticated or conditional access for a set time period, such as a guest or contractor endpoint, or employees leveraging webauth for network access. After the allowed connect grace period, they must be fully reauthenticated and registered.

- **PurgeDate**—Date to purge the endpoint.
  - This option can be used for special events or groups where access is granted for a specific time, regardless of creation or start time. This allows all endpoints to be purged at same time. For example,
a trade show, a conference, or a weekly training class with new members each week, where access is granted for specific week or month rather than absolute days/weeks/months.
PART IV

Manage Users and End-User Portals

• Manage Users and External Identity Sources, on page 309
• Configure Guest Access, on page 443
• Support Device Access, on page 495
• Customize End-User Web Portals, on page 519
Manage Users and External Identity Sources

- Cisco ISE Users, on page 309
- Internal and External Identity Sources, on page 319
- Certificate Authentication Profiles, on page 322
- Active Directory as an External Identity Source, on page 323
- Active Directory Requirements to Support Easy Connect and Passive Identity services, on page 345
- Easy Connect, on page 355
- PassiveID Work Center, on page 359
- LDAP, on page 409
- ODBC Identity Source, on page 417
- RADIUS Token Identity Sources, on page 423
- RSA Identity Sources, on page 428
- SAMLv2 Identity Provider as an External Identity Source, on page 433
- Identity Source Sequences, on page 438
- Identity Source Details in Reports, on page 440

Cisco ISE Users

In this chapter, the term user refers to employees and contractors who access the network regularly as well as sponsor and guest users. A sponsor user is an employee or contractor of the organization who creates and manages guest-user accounts through the sponsor portal. A guest user is an external visitor who needs access to the organization’s network resources for a limited period of time.

You must create an account for any user to gain access to resources and services on the Cisco ISE network. Employees, contractors, and sponsor users are created from the Admin portal.

User Identity

User identity is like a container that holds information about a user and forms their network access credentials. Each user’s identity is defined by data and includes: a username, e-mail address, password, account description, associated administrative group, user group, and role.
User Groups

User groups are a collection of individual users who share a common set of privileges that allow them to access a specific set of Cisco ISE services and functions.

User Identity Groups

A user’s group identity is composed of elements that identify and describe a specific group of users that belong to the same group. A group name is a description of the functional role that the members of this group have. A group is a listing of the users that belong to this group.

Default User Identity Groups

Cisco ISE comes with the following predefined user identity groups:

- Employee—Employees of your organization belong to this group.
- SponsorAllAccount—Sponsor users who can suspend or reinstate all guest accounts in the Cisco ISE network.
- SponsorGroupAccounts—Sponsor users who can suspend guest accounts created by sponsor users from the same sponsor user group.
- SponsorOwnAccounts—Sponsor users who can only suspend the guest accounts that they have created.
- Guest—A visitor who needs temporary access to resources in the network.
- ActivatedGuest—A guest user whose account is enabled and active.

User Role

A user role is a set of permissions that determine what tasks a user can perform and what services they can access on the Cisco ISE network. A user role is associated with a user group. For example, a network access user.

User Account Custom Attributes and Password Policies

Cisco ISE allows you to restrict a user’s network access based on user attributes. Cisco ISE comes with a set of predefined user attributes and also allows you to create custom attributes. Both types of attributes can be used in conditions that define the authentication policy. You can also define a password policy for user accounts so that passwords meet specified criteria.

Custom User Attributes

You can configure additional user-account attributes on the User Custom Attributes page (Administration > Identity Management > Settings > User Custom Attributes). You can also view the list of predefined user attributes on this page. You cannot edit the predefined user attributes.

Enter the required details on the User Custom Attributes pane to add a new custom attribute. The custom attributes and the default values that you add on the User Custom Attributes page are displayed while adding or editing a Network Access user (Administration > Identity Management > Identities > Users > Add/Edit)
or Admin user (Administration > System > Admin Access > Administrators > Admin Users > Add/Edit). You can change the default values while adding or editing a Network Access or Admin user.

You can select the following data types for the custom attributes on the User Custom Attributes page:

- **String**—You can specify the maximum string length (maximum allowed length for a string attribute value).
- **Integer**—You can configure the minimum and maximum value (specifies the lowest and the highest acceptable integer value).
- **Enum**—You can specify the following values for each parameter:
  - Internal value
  - Display value

You can also specify the default parameter. The values that you add in the Display field are displayed while adding or editing a Network Access or Admin user.

- **Float**
- **Password**—You can specify the maximum string length.
- **Long**—You can configure the minimum and maximum value.
- **IP**—You can specify a default IPv4 or IPv6 address.
- **Boolean**—You can set either True or False as the default value.
- **Date**—You can select a date from the calendar and set it as the default value. The date is displayed in yyyy-mm-dd format.

Check the Mandatory check box if you want to make an attribute mandatory while adding or editing a Network Access or Admin user. You can also set default values for the custom attributes.

The custom attributes can be used in the authentication policies. The data type and the allowable range that you set for the custom attributes will be applied for the custom attribute values in the policy conditions.

**User Authentication Settings**

You can define the criteria that user-account passwords must meet in the User Authentication Settings page. Choose Administration > Identity Management > Settings > User Authentication Settings > Password Policy.

The following table describes the fields in the Password Policy page.

**Table 12: User Password Policy Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum length</td>
<td>Sets the minimum length of the password (in characters)</td>
</tr>
<tr>
<td>Fields</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password must not contain</td>
<td>User name—Restricts the use of the username or its characters in reverse order</td>
</tr>
<tr>
<td></td>
<td>“cisco”—Restricts the use of “cisco” or its characters in reverse order</td>
</tr>
<tr>
<td></td>
<td>This word—Restricts the use of any word that you define or its characters in reverse order.</td>
</tr>
<tr>
<td></td>
<td>Repeated characters four or more times consecutively—Restricts the use of characters repeated four or more times consecutively</td>
</tr>
<tr>
<td></td>
<td>Dictionary words—Check this check box to restrict the use of any dictionary word, its characters in reverse order or its letters replaced with other characters.</td>
</tr>
<tr>
<td></td>
<td>Substitution of &quot;s&quot;, &quot;@&quot; for &quot;a&quot;, &quot;0&quot; for &quot;o&quot;, &quot;1&quot; for &quot;l&quot;, &quot;!&quot; for &quot;i&quot;, &quot;3&quot; for &quot;e&quot;, is not permitted. For example, Pa$$w0rd</td>
</tr>
<tr>
<td></td>
<td>• Default Dictionary—Choose this option to use the default Linux dictionary in Cisco ISE. The default dictionary contains approximately 480,000 English words. By default, this option is selected.</td>
</tr>
<tr>
<td></td>
<td>• Custom Dictionary—Choose this option to use your customized dictionary. Click <strong>Choose File</strong> to select the custom dictionary file. The text file must be of newline-delimited words, .dic extension, and size less than 20 MB.</td>
</tr>
</tbody>
</table>
Generate Automatic Password for Users and Administrators

Cisco ISE introduces a Generate Password option on the user and administrator creation page to generate instant password adhering to Cisco ISE password policies. This helps the users or administrators to use the password generated by Cisco ISE than spending time in thinking of a safe password to be configured.

The Generate Password option is available in the following three locations of Cisco ISE web interface:

- Users—Administration > Identity Management > Identities > Users.
- Logged in Administrator(Current Administrator)—Settings > Account Settings > Change Password.

Add Users

Cisco ISE allows you to view, create, modify, duplicate, delete, change the status, import, export, or search for attributes of Cisco ISE users.
If you are using a Cisco ISE internal database, you must create an account for any new user who needs access to resources or services on a Cisco ISE network.

**Step 1** Choose Administration > Identity Management > Identities > Users.
You can also create users by accessing the Work Centers > Device Administration > Identities > Users page.

**Step 2** Click Add (+) to create a new user.

**Step 3** Enter values for the fields.
Do not include space, +, and * characters in the username. If you use the Cisco ISE Internal Certificate Authority (CA) for BYOD, the username that you provide here is used as the Common Name for the endpoint certificate. Cisco ISE Internal CA does not support "+" or "*" characters in the Common Name field.

**Step 4** Click Submit to create a new user in the Cisco ISE internal database.

---

**Export Cisco ISE User Data**

You might have to export user data from the Cisco ISE internal database. Cisco ISE allows you to export user data in the form of a password-protected csv file.

**Step 1** Choose Administration > Identity Management > Identities > Users.

**Step 2** Check the check box that corresponds to the user(s) whose data you want to export.

**Step 3** Click Export Selected.

**Step 4** Enter a key for encrypting the password in the Key field.

**Step 5** Click Start Export to create a users.csv file.

**Step 6** Click OK to export the users.csv file.

---

**Import Cisco ISE Internal Users**

You can import new user data into ISE with a csv file to create new internal accounts. A template csv file is available for download on the pages where you can import user accounts. You can import users on Administration > Identity Management > Identities > Users. Sponsors can import users on the Sponsor portal. The Sponsor Portal Guide tells Sponsors how to import guest accounts. See Configure Account Content for Sponsor Account Creation, on page 480 for information about configuring the information types that the sponsor guest accounts use.

---

**Note**
If the csv file contains custom attributes, the data type and the allowable range that you set for the custom attributes will be applied for the custom attribute values during import.

**Step 1** Choose Administration > Identity Management > Identities > Users.

**Step 2** Click Import to import users from a comma-delimited text file.
If you do not have a comma-delimited text file, click **Generate a Template** to create a csv file with the heading rows filled in.

**Step 3** In the File text box, enter the filename containing the users to import, or click **Browse** and navigate to the location where the file resides.

**Step 4** Check the **Create new user(s) and update existing user(s) with new data** checkboxes if you want to both create new users and update existing users.

**Step 5** Click **Save** to save your changes to the Cisco ISE internal database.

---

**Note**

We recommend that you do not delete all the network access users at a time, because this may lead to CPU spike and the services to crash, especially if you are using a very large database.

---

### Create a User Identity Group

You must create a user identity group before you can assign a user to it.

**Step 1** Choose **Administration > Identity Management > Groups > Identity Groups > User Identity Groups > Add**.

You can also create a user identity group by accessing the **Work Centers > Device Administration > User Identity Groups > Identity Groups > User Identity Groups > Add** page.

**Step 2** Enter values in the Name and Description fields. Supported characters for the Name field are space $ & ' ( ) * + - . / @ _ .

**Step 3** Click **Submit**.

---

**Related Topics**

- User Groups, on page 310
- User Identity Groups, on page 310
- Default User Identity Groups
- Import User Identity Groups, on page 316

### Export User Identity Groups

Cisco ISE allows you to export locally configured user identity groups in the form of a csv file.

**Step 1** Choose **Administration > Identity Management > Groups > Identity Groups > User Identity Groups**.

**Step 2** Check the check box that corresponds to the user identity group that you want to export, and click **Export**.

**Step 3** Click **OK**.
**Import User Identity Groups**

Cisco ISE allows you to import user identity groups in the form of a csv file.

---

**Step 1** Choose Administration > Identity Management > Groups > Identity Groups > User Identity Groups.

**Step 2** Click Generate a Template to get a template to use for the import file.

**Step 3** Click Import to import network access users from a comma-delimited text file.

**Step 4** Check the Overwrite existing data with new data check box if you want to both add a new user identity group and update existing user identity groups.

**Step 5** Click Import.

**Step 6** Click Save to save your changes to the Cisco ISE database.

---

**Configure Maximum Concurrent Sessions**

For optimal performance, you can limit the number of concurrent user sessions. You can set the limits at the user level or at the group level. Depending upon the maximum user session configurations, the session count is applied to the user.

You can configure the maximum number of concurrent sessions for each user per ISE node. Sessions above this limit are rejected.

---

**Step 1** Choose Administration > System > Settings > Max Sessions > User.

**Step 2** Do one of the following:

- Enter the maximum number of concurrent sessions that are allowed for each user in the Maximum Sessions per User field.

  Or

- Check the Unlimited Sessions check box if you want the users to have unlimited sessions. This option is selected by default.

**Step 3** Click Save.

If the maximum number of sessions is configured at both the user and group level, the smaller value will have precedence. For example, if the maximum session value for a user is set as 10 and the maximum session value of the group to which the user belongs is set as 5, the user can have a maximum of 5 sessions only.

If you configure the maximum sessions to 1, and the WLC the user connects with is not running a supported version of WLC, then users gets an error telling them to disconnect and reconnect again.

**Maximum Concurrent Sessions for a Group**

You can configure the maximum number of concurrent sessions for the identity groups.

Sometimes all the sessions can be used by a few users in the group. Requests from other users to create a new session are rejected because the number of sessions has already reached the maximum configured value. Cisco ISE allows you to configure a maximum session limit for each user in the group; each user belonging to a
specific identity group cannot open sessions more than the session limit, irrespective of the number of sessions other users from the same group have opened. When calculating the session limit for a particular user, the lowest configuration value takes the precedence—whether the global session limit per user, the session limit per identity group that the user belongs to, or the session limit per user in the group.

To configure maximum number of concurrent sessions for an identity group:

**Step 1** Choose Administration > System > Settings > Max Sessions > Group.

All the configured identity groups are listed.

**Step 2** Click the Edit icon next to the group that you want to edit and enter the values for the following:

- Maximum number of concurrent sessions permitted for that group. If the maximum number of sessions for a group is set as 100, the total count of all sessions established by all members of that group cannot exceed 100.
  
  **Note** Group-level session limits are applied based on the group hierarchy.

- Maximum number of concurrent sessions permitted for each user in that group. This option overrides the maximum number of sessions for a group.

If you want to set the maximum number of concurrent sessions for a group or maximum concurrent sessions for the users in a group as Unlimited, leave the Max Sessions for Group/Max Sessions for User in Group field blank, click the Tick icon, and then click Save. By default, both these values are set as Unlimited.

**Step 3** Click Save.

---

**Configure Counter Time Limit**

You can configure the timeout value for concurrent user sessions.

**Step 1** Choose Administration > System > Settings > Max Sessions > Counter Time Limit.

**Step 2** Select one of the following options:

- Unlimited—Check this check box if you do not want to set any timeout or time limit for the sessions.

- Delete sessions after—You can enter the timeout value for concurrent sessions in minutes, hours, or days. When a session exceeds the time limit, Cisco ISE deletes the session from the counter and updates the session count, thereby allowing new sessions. Users will not be logged out if their sessions exceed the time limit.

**Step 3** Click Save.

You can reset the session count from the RADIUS Live Logs page. Click the Actions icon displayed on the Identity, Identity Group, or Server column to reset the session count. When you reset a session, the session is deleted from the counter (thereby allowing new sessions). Users will not be disconnected if their sessions are deleted from the counter.
Account Disable Policy

Cisco ISE introduces the account disable policy for users and administrators to achieve parity with Cisco Secure ACS. While authenticating or querying a user or administrator, Cisco ISE checks the global account disable policy settings at Administration > Identity Management > Settings > User Authentication Settings page and authenticates or returns a result based on the configuration.

Cisco ISE verifies the following three policies:

• Disable user accounts that exceed a specified date (yyyy-mm-dd)—Disables the user account on the specified date. However, the account disable policy settings for an individual network access user configured at Administration > Identity Management > Identities > Users > Account Disable Policy takes precedence over the global settings.

• Disable user account after $n$ days of account creation or last enable—Disables user accounts after specific number of days of account creation or the last date when the account was active. You can check the user status at Administration > Identity Management > Identities > Users > Status.

• Disable accounts after $n$ days of inactivity—Disables administrator and user accounts that have not been authenticated for the configured consecutive number of days.

When you migrate from Cisco Secure ACS to Cisco ISE, the account disable policy settings specified for a network access user in Cisco Secure ACS is migrated to Cisco ISE.

Disable Individual User Accounts

Cisco ISE allows you to disable the user account for each individual user if the disable account date exceeds the date specified by the admin user.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Administration &gt; Identity Management &gt; Identities &gt; Users.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Add to create a new user or check the check box next to an existing user and click Edit to edit the existing user details.</td>
</tr>
</tbody>
</table>
| Step 3 | Check the Disable account if the date exceeds check box and select the date.  
This option allows you to disable the user account when the configured date exceeds at user level. You can configure different expiry dates for different users as required. This option overrules the global configuration for each individual user. The configured date can either be the current system date or a future date.  
**Note** You are not allowed to enter a date earlier than the current system date. |
| Step 4 | Click Submit to configure the account disable policy for an individual user. |

Disable User Accounts Globally

Cisco ISE allows you to disable user accounts on a certain date, a number of days after account creation or last access date, and after a number of days of account inactivity.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Administration &gt; Identity Management &gt; Settings &gt; User Authentication Settings &gt; Account Disable Policy.</td>
</tr>
</tbody>
</table>
Step 2  Perform one of the following actions:

• Check the **Disable account if date exceeds** check box and select the appropriate date in yyyy-mm-dd format. This option allows you to disable the user account when the configured date is exceeded. However, the **Disable account if date exceeds** option at user level takes precedence over the global configuration.

• Check the **Disable account after n days of account creation or last enable** check box and enter the number of days. This option allows you to disable the user account when the account creation date or last access date exceeds the specified number of days. Administrators can manually enable the disabled user accounts and the number of days count is automatically reset after enabling the user accounts.

• Check the **Disable account after n days of inactivity** check box and enter the number of days. This option allows you to disable the user account when the account is inactive for the specified number of days.

Step 3  Click **Submit** to configure the global account disable policy.

---

**Internal and External Identity Sources**

Identity sources contain user information that Cisco ISE uses to validate credentials during user authentication, and to retrieve group information and other attributes that are associated with the user for use in authorization policies. They are databases that store user information in the form of records. You can add, edit, and delete user information from identity sources.

Cisco ISE supports internal and external identity sources. Both sources can be used as an authentication source for sponsor-user and guest-user authentication.

**Internal Identity Sources**

Cisco ISE has an internal user database that you can use to store user information. Users in the internal user database are called internal users. Cisco ISE also has an internal endpoint database that stores information about all the devices and endpoints that connect to it.

**External Identity Sources**

Cisco ISE allows you to configure the external identity source that contains user information. Cisco ISE connects to an external identity source to obtain user information for authentication. External identity sources also include certificate information for the Cisco ISE server and certificate authentication profiles. Cisco ISE uses authentication protocols to communicate with external identity sources. The following table lists authentication protocols and the external identity sources that they support.

Note the following points while configuring policies for internal users:

• Configure an authentication policy to authenticate internal users against an internal identity store.

• Configure an authorization policy for internal user groups by selecting the following option:

  **Identitygroup.Name EQUALS User Identity Groups: Group_Name**
### Table 13: Authentication Protocols and Supported External Identity Sources

<table>
<thead>
<tr>
<th>Protocol (Authentication Type)</th>
<th>Internal Database</th>
<th>Active Directory</th>
<th>LDAP</th>
<th>RADIUS Token Server or RSA</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP-GTC, PAP (plain text password)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MS-CHEAP password hash: MSCHAPv1/v2 EAP-MSCHAPv2 (as inner method of PEAP, EAP-FAST, or EAP-TTLS) LEAP</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>EAP-MD5 CHAP</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>EAP-TLS PEAP-TLS (certificate retrieval)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

**Note**
For TLS authentications (EAP-TLS and PEAP-TLS), identity sources are not required but can optionally be added for authorization policy conditions.

---

### Create an External Identity Source

Cisco ISE can connect with external identity sources such as Active Directory, LDAP, RADIUS Token, and RSA SecurID servers to obtain user information for authentication and authorization. External identity sources also include certificate authentication profiles that you need for certificate-based authentications.
To work with passive identity services, which enable you to receive and share authenticated user identities, see Additional Passive Identity Service Providers, on page 368.

**Step 1**

Choose Administration > Identity Management > External Identity Sources.

**Step 2**

Choose one of these options:

- **Certificate Authentication Profile** for certificate-based authentications.
- **Active Directory** to connect to an Active Directory as an external identity source. See Active Directory as an External Identity Source, on page 323 for more details.
- **LDAP** to add an LDAP identity source. See LDAP, on page 409 for more details.
- **RADIUS Token** to add a RADIUS Token server. See RADIUS Token Identity Sources, on page 423 for more details.
- **RSASecurID** to add an RSA SecurID server. See RSA Identity Sources, on page 428 for more details.
- **SAML Id Providers** to add an identity provider (IdP), such as Oracle Access Manager. See SAMLv2 Identity Provider as an External Identity Source, on page 433 for more details.
- **Social Login** to add a Social Login, such as Facebook, as an external identity source, see Social Login for Self-Registered Guests, on page 456.

**Related Topics**

- Internal and External Identity Sources, on page 319
- Internal Identity Sources
- External Identity Sources
- Add a Certificate Authentication Profile, on page 322
- Configure Active Directory as an External Identity Source, on page 328
- Support for Active Directory Multi-Join Configuration, on page 335
- Add LDAP Identity Sources, on page 414
- Add a RADIUS Token Server, on page 426
- Add RSA Identity Sources, on page 430
- Identity Source Sequences, on page 438
- Create Identity Source Sequences, on page 439
- Identity Source Details in Reports, on page 440
- authentications Dashlet, on page 440
- Identity Source Reports, on page 441

**Authenticate Internal User Against External Identity Store Password**

Cisco ISE allows you to authenticate internal users against external identity store passwords. Cisco ISE provides an option to select the password identity store for internal users from the Administration > Identity Management > Identities > Users page. Administrators can select the identity store from the list of Cisco ISE External Identity Sources while adding or editing users in the Users page. The default password identity store for an internal user is the internal identity store. Cisco Secure ACS users will retain the same password identity store during and after migration from Cisco Secure ACS to Cisco ISE. When you upgrade from earlier versions of Cisco ISE to Cisco ISE 2.1, Cisco ISE 2.1 sets the internal identity store as the default identity store for all internal users.
Cisco ISE supports the following external identity stores for password types:

- Active Directory
- LDAP
- ODBC
- RADIUS Token server
- RSA SecurID server

**Certificate Authentication Profiles**

For each profile, you must specify the certificate field that should be used as the principal username and whether you want a binary comparison of the certificates.

**Add a Certificate Authentication Profile**

You must create a certificate authentication profile if you want to use the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) certificate-based authentication method. Instead of authenticating via the traditional username and password method, Cisco ISE compares a certificate received from a client with one in the server to verify the authenticity of a user.

**Before you begin**

You must be a Super Admin or System Admin.

---

**Step 1** Choose Administration > Identity Management > External Identity Sources > Certificate Authentication Profile > Add.

**Step 2** Enter the name and an optional description for the certificate authentication profile.

**Step 3** Select an identity store from the drop-down list.

Basic certificate checking does not require an identity source. If you want binary comparison checking for the certificates, you must select an identity source. If you select Active Directory as an identity source, subject and common name and subject alternative name (all values) can be used to look up a user.

**Step 4** Select the use of identity from **Certificate Attribute** or **Any Subject or Alternative Name Attributes in the Certificate**. This will be used in logs and for lookups.

If you choose **Any Subject or Alternative Name Attributes in the Certificate**, Active Directory UPN will be used as the username for logs and all subject names and alternative names in a certificate will be tried to look up a user. This option is available only if you choose Active Directory as the identity source.

**Step 5** Choose when you want to **Match Client Certificate Against Certificate In Identity Store**. For this you must select an identity source (LDAP or Active Directory.) If you select Active Directory, you can choose to match certificates only to resolve identity ambiguity.

- **Never**—This option never performs a binary comparison.
• Only to resolve identity ambiguity—This option performs the binary comparison of client certificate to certificate on account in Active Directory only if ambiguity is encountered. For example, several Active Directory accounts matching to identity names from certificate are found.

• Always perform binary comparison—This option always performs the binary comparison of client certificate to certificate on account in identity store (Active Directory or LDAP).

**Step 6**  
Click **Submit** to add the certificate authentication profile or save the changes.

---

**Active Directory as an External Identity Source**

Cisco ISE uses Microsoft Active Directory as an external identity source to access resources such as users, machines, groups, and attributes. User and machine authentication in Active Directory allows network access only to users and devices that are listed in Active Directory.

**ISE Community Resource**

ISE Administrative Portal Access with AD Credentials Configuration Example

---

**Active Directory Supported Authentication Protocols and Features**

Active Directory supports features such as user and machine authentications, changing Active Directory user passwords with some protocols. The following table lists the authentication protocols and the respective features that are supported by Active Directory.

**Table 14: Authentication Protocols Supported by Active Directory**

<table>
<thead>
<tr>
<th>Authentication Protocols</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP-FAST and password based Protected Extensible Authentication Protocol (PEAP)</td>
<td>User and machine authentication with the ability to change passwords using EAP-FAST and PEAP with an inner method of MS-CHAPv2 and EAP-GTC</td>
</tr>
<tr>
<td>Password Authentication Protocol (PAP)</td>
<td>User and machine authentication</td>
</tr>
<tr>
<td>Microsoft Challenge Handshake Authentication Protocol Version 1 (MS-CHAPv1)</td>
<td>User and machine authentication</td>
</tr>
<tr>
<td>Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2)</td>
<td>User and machine authentication</td>
</tr>
<tr>
<td>Extensible Authentication Protocol-Generic Token Card (EAP-GTC)</td>
<td>User and machine authentication</td>
</tr>
<tr>
<td>Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)</td>
<td>• User and machine authentication</td>
</tr>
<tr>
<td></td>
<td>• Groups and attributes retrieval</td>
</tr>
<tr>
<td></td>
<td>• Binary certificate comparison</td>
</tr>
</tbody>
</table>
### Authentication Protocols

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Features</th>
</tr>
</thead>
</table>
| Extensible Authentication Protocol - Flexible Authentication via Secure Tunneling-Transport Layer Security (EAP-FAST-TLS) | • User and machine authentication  
• Groups and attributes retrieval  
• Binary certificate comparison |
| Protected Extensible Authentication Protocol - Transport Layer Security (PEAP-TLS) | • User and machine authentication  
• Groups and attributes retrieval  
• Binary certificate comparison |
| Lightweight Extensible Authentication Protocol (LEAP) | User authentication |

**Active Directory Attribute and Group Retrieval for Use in Authorization Policies**

Cisco ISE retrieves user or machine attributes and groups from Active Directory for use in authorization policy rules. These attributes can be used in Cisco ISE policies and determine the authorization level for a user or machine. Cisco ISE retrieves user and machine Active Directory attributes after successful authentication and can also retrieve attributes for an authorization that is independent of authentication.

Cisco ISE may use groups in external identity stores to assign permissions to users or computers; for example, to map users to sponsor groups. You should note the following restrictions on group memberships in Active Directory:

- Policy rule conditions may reference any of the following: a user’s or computer’s primary group, the groups of which a user or computer is a direct member, or indirect (nested) groups.
- Domain local groups outside a user’s or computer’s account domain are not supported.

**Note**

You can use the value of the Active Directory attribute, `msRadiusFramedIPAddress`, as an IP address. This IP address can be sent to a network access server (NAS) in an authorization profile. The `msRadiusFramedIPAddress` attribute supports only IPv4 addresses. Upon user authentication, the `msRadiusFramedIPAddress` attribute value fetched for the user will be converted to IP address format.

Attributes and groups are retrieved and managed per join point. They are used in authorization policy (by selecting first the join point and then the attribute). You cannot define attributes or groups per scope for authorization, but you can use scopes for authentication policy. When you use a scope in authentication policy, it is possible that a user is authenticated via one join point, but attributes and/or groups are retrieved via another join point that has a trust path to the user's account domain. You can use authentication domains to ensure that no two join points in one scope have any overlap in authentication domains.

**Note**

An authorization policy fails if the rule contains an Active Directory group name with special characters such as /, !, @, \, $, %, ^, &, *, (,), _, +, or ~.

**Use Explicit UPN**

To reduce ambiguity when matching user information against Active Directory's User-Principal-Name (UPN) attributes, you must configure Active Directory to use Explicit UPN. Using Implicit UPN can produce ambiguous results if two users have the same value for `sAMAccountName`.

To set Explicit UPN in Active Directory, open the Advanced Tuning page, and set the attribute `REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\UseExplicitUPN` to 1.

### Support for Boolean Attributes

Cisco ISE supports retrieving Boolean attributes from Active Directory and LDAP identity stores.

You can configure the Boolean attributes while configuring the directory attributes for Active Directory or LDAP. These attributes are retrieved upon authentication with Active Directory or LDAP.

The Boolean attributes can be used for configuring policy rule conditions.

The Boolean attribute values are fetched from Active Directory or LDAP server as String type. Cisco ISE supports the following values for the Boolean attributes:

<table>
<thead>
<tr>
<th>Boolean attribute</th>
<th>Supported values</th>
</tr>
</thead>
<tbody>
<tr>
<td>True</td>
<td>t, T, true, TRUE, True, 1</td>
</tr>
<tr>
<td>False</td>
<td>f, F, false, FALSE, False, 0</td>
</tr>
</tbody>
</table>

**Note**

Attribute substitution is not supported for the Boolean attributes.

If you configure a Boolean attribute (for example, `msTSAllowLogon`) as String type, the Boolean value of the attribute in the Active Directory or LDAP server will be set for the String attribute in Cisco ISE. You can change the attribute type to Boolean or add the attribute manually as Boolean type.

### Active Directory Certificate Retrieval for Certificate-Based Authentication

Cisco ISE supports certificate retrieval for user and machine authentication that uses the EAP-TLS protocol. The user or machine record on Active Directory includes a certificate attribute of the binary data type. This certificate attribute can contain one or more certificates. Cisco ISE identifies this attribute as `userCertificate` and does not allow you to configure any other name for this attribute. Cisco ISE retrieves this certificate and uses it to perform binary comparison.

The certificate authentication profile determines the field where the username is taken from in order to lookup the user in Active Directory to be used for retrieving certificates, for example, Subject Alternative Name (SAN) or Common Name. After Cisco ISE retrieves the certificate, it performs a binary comparison of this certificate with the client certificate. When multiple certificates are received, Cisco ISE compares the certificates to check for one that matches. When a match is found, the user or machine authentication is passed.
Active Directory User Authentication Process Flow

When authenticating or querying a user, Cisco ISE checks the following:

- MS-CHAP and PAP authentications check if the user is disabled, locked out, expired or out of logon hours and the authentication fails if some of these conditions are true.

- EAP-TLS authentications checks if the user is disabled or locked out and the authentication fails if some of these conditions is met.

Support for Active Directory Multidomain Forests

Cisco ISE supports Active Directory with multidomain forests. Within each forest, Cisco ISE connects to a single domain, but can access resources from the other domains in the Active Directory forest if trust relationships are established between the domain to which Cisco ISE is connected and the other domains.

Refer to Release Notes for Cisco Identity Services Engine for a list of Windows Server Operating Systems that support Active Directory services.

---

Note

Cisco ISE does not support Microsoft Active Directory servers that reside behind a network address translator and have a Network Address Translation (NAT) address.

---

Prerequisites for Integrating Active Directory and Cisco ISE

This section describes the manual steps necessary in order to configure Active Directory for integration with Cisco ISE. However, in most cases, you can enable Cisco ISE to automatically configure Active Directory. The following are the prerequisites to integrate Active Directory with Cisco ISE.

- Ensure you have Active Directory Domain Admin credentials, required in order to make changes to any of the AD domain configurations.

- Ensure you have the privileges of a Super Admin or System Admin in ISE.

- Use the Network Time Protocol (NTP) server settings to synchronize the time between the Cisco ISE server and Active Directory. You can configure NTP settings from Cisco ISE CLI.

- Cisco ISE can connect with multiple Active Directory domains that do not have a two-way trust or have zero trust between them. If you want to query other domains from a specific join point, ensure that trust relationships exist between the join point and the other domains that have user and machine information to which you need access. If trust relationships does not exist, you must create another join point to the untrusted domain. For more information on establishing trust relationships, refer to Microsoft Active Directory documentation.

- You must have at least one global catalog server operational and accessible by Cisco ISE, in the domain to which you are joining Cisco ISE.
Active Directory Account Permissions Required for Performing Various Operations

<table>
<thead>
<tr>
<th>Join Operations</th>
<th>Leave Operations</th>
<th>Cisco ISE Machine Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>For the account that is used to perform the join operation, the following permissions are required:</td>
<td>For the account that is used to perform the leave operation, the following permissions are required:</td>
<td>For the newly created Cisco ISE machine account that is used to communicate to the Active Directory connection, the following permissions are required:</td>
</tr>
<tr>
<td>• Search Active Directory (to see if a Cisco ISE machine account already exists)</td>
<td>• Search Active Directory (to see if a Cisco ISE machine account already exists)</td>
<td>• Ability to change own password</td>
</tr>
<tr>
<td>• Create Cisco ISE machine account to domain (if the machine account does not already exist)</td>
<td>• Remove Cisco ISE machine account from domain</td>
<td>• Read the user/machine objects corresponding to users/machines being authenticated</td>
</tr>
<tr>
<td>• Set attributes on the new machine account (for example, Cisco ISE machine account password, SPN, dnsHostname)</td>
<td>If you perform a force leave (leave without the password), it will not remove the machine account from the domain.</td>
<td>• Query some parts of the Active Directory to learn about required information (for example, trusted domains, alternative UPN suffixes and so on.)</td>
</tr>
<tr>
<td>It is not mandatory to be a domain administrator to perform a join operation.</td>
<td></td>
<td>• Ability to read tokenGroups attribute</td>
</tr>
</tbody>
</table>

**Note**

The credentials used for the join or leave operation are not stored in Cisco ISE. Only the newly created Cisco ISE machine account credentials are stored, and this is in order to enable the Endpoint probe to run as well.

Network Ports That Must Be Open for Communication

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port (remote-local)</th>
<th>Target</th>
<th>Authenticated</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS (TCP/UDP)</td>
<td>Random number greater than or equal to 49152</td>
<td>DNS Servers/AD Domain Controllers</td>
<td>No</td>
<td>—</td>
</tr>
</tbody>
</table>
### DNS Server

While configuring your DNS server, make sure that you take care of the following:

- The DNS servers that you configure in Cisco ISE must be able to resolve all forward and reverse DNS queries for the domains that you want to use.

- The Authoritative DNS server is recommended to resolve Active Directory records, as DNS recursion can cause delays and have significant negative impact on performance.

- All DNS servers must be able to answer SRV queries for DCs, GCs, and KDCs with or without additional Site information.

- Cisco recommends that you add the server IP addresses to SRV responses to improve performance.

- Avoid using DNS servers that query the public Internet. They can leak information about your network when an unknown name has to be resolved.

### Configure Active Directory as an External Identity Source

Configure Active Directory as an external identity source as part of the configuration for features such as Easy Connect and the PassiveID Work Center. For more information about these features, see Easy Connect, on page 355 and PassiveID Work Center, on page 359.

Before you configure Active Directory as an External Identity Source, make sure that:

- The Microsoft Active Directory server does not reside behind a network address translator and does not have a Network Address Translation (NAT) address.

- The Microsoft Active Directory account intended for the join operation is valid and is not configured with the Change Password on Next Login.

- You have the privileges of a Super Admin or System Admin in ISE.
If you see operational issues when Cisco ISE is connected to Active Directory, see the AD Connector Operations Report under **Operations > Reports**.

You must perform the following tasks to configure Active Directory as an external identity source.

1. Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point, on page 329
2. Configure Authentication Domains, on page 332
3. Configure Active Directory User Groups, on page 333
4. Configure Active Directory User and Machine Attributes, on page 333
5. (Optional) Modify Password Changes, Machine Authentications, and Machine Access Restriction Settings, on page 334

**Related Topics**
- Active Directory as an External Identity Source, on page 323
- Active Directory Supported Authentication Protocols and Features, on page 323
- Active Directory Attribute and Group Retrieval for Use in Authorization Policies, on page 324
- Active Directory Certificate Retrieval for Certificate-Based Authentication, on page 325
- Active Directory User Authentication Process Flow, on page 326
- Support for Active Directory Multidomain Forests, on page 326
- Support for Active Directory Multi-Join Configuration, on page 335
- Active Directory Key Features in Cisco ISE 2.x
- Guidelines for Setting Up Active Directory as an External Identity Source
- Diagnose Active Directory Problems, on page 340
- Enable Active Directory Debug Logs, on page 341
- Obtain the Active Directory Log File for Troubleshooting, on page 341
- Active Directory Advanced Tuning, on page 342

**Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point**

**Before you begin**

Make sure that the Cisco ISE node can communicate with the networks where the NTP servers, DNS servers, domain controllers, and global catalog servers are located. You can check these parameters by running the Domain Diagnostic tool.

Join points must be created in order to work with Active Directory as well as with the Agent, Syslog, SPAN and Endpoint probes of the Passive ID Work Center.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Administration &gt; Identity Management &gt; External Identity Sources &gt; Active Directory.</strong></td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>Add</strong> and enter the domain name and identity store name from the Active Directory Join Point Name settings.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Submit</strong>. A pop-up appears asking if you want to join the newly created join point to the domain. Click <strong>Yes</strong> if you want to join immediately.</td>
</tr>
</tbody>
</table>
If you clicked No, then saving the configuration saves the Active Directory domain configuration globally (in the primary and secondary policy service nodes), but none of the Cisco ISE nodes are joined to the domain yet.

**Step 4**
Check the checkbox next to the new Active Directory join point that you created and click Edit, or click on the new Active Directory join point from the navigation pane on the left. The deployment join/leave table is displayed with all the Cisco ISE nodes, the node roles, and their status.

**Step 5**
Check the checkbox next to the relevant Cisco ISE nodes and click Join to join the Cisco ISE node to the Active Directory domain.

You must do this explicitly even though you saved the configuration. To join multiple Cisco ISE nodes to a domain in a single operation, the username and password of the account to be used must be the same for all join operations. If different usernames and passwords are required to join each Cisco ISE node, the join operation should be performed individually for each Cisco ISE node.

**Step 6**
Enter the Active Directory username and password from the Join Domain dialog box that opens.

It is strongly recommended that you choose Store credentials, in which case your administrator's user name and password will be saved in order to be used for all Domain Controllers (DC) that are configured for monitoring.

The user used for the join operation should exist in the domain itself. If it exists in a different domain or subdomain, the username should be noted in a UPN notation, such as jdoe@acme.com.

**Step 7**
(Optional) Check the Specify Organizational Unit checkbox.

You should check this checkbox in case the Cisco ISE node machine account is to be located in a specific Organizational Unit other than CN=Computers,DC=someDomain,DC=someTLD. Cisco ISE creates the machine account under the specified organizational unit or moves it to this location if the machine account already exists. If the organizational unit is not specified, Cisco ISE uses the default location. The value should be specified in full distinguished name (DN) format. The syntax must conform to the Microsoft guidelines. Special reserved characters, such as /+,;<=<> line feed, space, and carriage return must be escaped by a backslash (\). For example, OU=Cisco ISE,US,OU=IT Servers,OU=Servers, and Workstations,DC=someDomain,DC=someTLD. If the machine account is already created, you need not check this checkbox. You can also change the location of the machine account after you join to the Active Directory domain.

**Step 8**
Click OK.

You can select more than one node to join to the Active Directory domain.

If the join operation is not successful, a failure message appears. Click the failure message for each node to view detailed logs for that node.

**Note**
When the join is complete, Cisco ISE updates its AD groups and corresponding SIDS. Cisco ISE automatically starts the SID update process. You must ensure that this process is allowed to complete.

**Note**
You might not be able to join Cisco ISE with an Active Directory domain if the DNS SRV records are missing (the domain controllers do not advertise their SRV records for the domain that you are trying to join to). Refer to the following Microsoft Active Directory documentation for troubleshooting information:

- [http://support.microsoft.com/kb/816587](http://support.microsoft.com/kb/816587)

---

**What to do next**

Configure Active Directory User Groups, on page 333
Configure authentication domains.

**Add Domain Controllers**

**Step 1** Choose **Work Centers > PassiveID > Providers** and then from the left panel choose **Active Directory**.

**Step 2** Check the check box next to the Active Directory join point that you created and click **Edit**. The deployment join/leave table is displayed with all the Cisco ISE nodes, the node roles, and their statuses.

**Step 3** Note: To add a new Domain Controller (DC) for Passive Identity services, you need the login credentials of that DC.

Go to the PassiveID tab and click **Add DCs**.

**Step 4** Check the check box next to the domain controllers that you would like to add to the join point for monitoring and click **OK**.

The domain controllers appear in the Domain Controllers list of the PassiveID tab.

**Step 5** Configure the domain controller:

a) Checkmark the domain controller and click **Edit**. The **Edit Item** screen appears.

b) Optionally, edit the different domain controller fields. For more information, see **Active Directory Settings, on page 365**.

c) If you selected WMI protocol, click **Configure** to configure WMI automatically and click **Test** to test the connection.

For more information about automatically configuring WMI, see **Configure WMI, on page 331**.

**Configure WMI**

**Before you begin**

Ensure you have Active Directory Domain Admin credentials, required in order to make changes to any of the AD domain configurations.

**Step 1** Choose **Administration > Identity Management > External Identity Sources > Active Directory**.

**Step 2** Check the checkbox next to the Active Directory join point that you created and click **Edit**. The deployment join/leave table is displayed with all the Cisco ISE nodes, the node roles, and their statuses. For more information, see **Table 17: Active Directory Join/Leave Table, on page 366**.

**Step 3** Go to the Passive ID tab, check the check box next to the relevant domain controllers and click **Config WMI** to enable ISE to automatically configure the domain controllers you selected.

To configure Active Directory and Domain Controllers manually, or to troubleshoot any problems with configuration, see **Prerequisites for Integrating Active Directory and Cisco ISE, on page 326**.

**Leave the Active Directory Domain**

If you no longer need to authenticate users or machines from this Active Directory domain or from this join point, you can leave the Active Directory domain.

When you reset the Cisco ISE application configuration from the command-line interface or restore configuration after a backup or upgrade, it performs a leave operation, disconnecting the Cisco ISE node from the Active Directory domain, if it is already joined. However, the Cisco ISE node account is not removed from the Active Directory domain. We recommend that you perform a leave operation from the Admin portal...
with the Active Directory credentials because it also removes the node account from the Active Directory
domain. This is also recommended when you change the Cisco ISE hostname.

Before you begin
If you leave the Active Directory domain, but still use Active Directory as an identity source for authentication
(either directly or as part of an identity source sequence), authentications may fail.

---

**Step 1** Choose Administration > Identity Management > External Identity Sources > Active Directory.

**Step 2** Check the checkbox next to the Active Directory join point that you created and click Edit. The deployment join/leave
table is displayed with all the Cisco ISE nodes, the node roles, and their statuses.

**Step 3** Check the checkbox next to the Cisco ISE node and click Leave.

**Step 4** Enter the Active Directory username and password, and click OK to leave the domain and remove the machine account
from the Cisco ISE database.

If you enter the Active Directory credentials, the Cisco ISE node leaves the Active Directory domain and deletes the
Cisco ISE machine account from the Active Directory database.

**Note** To delete the Cisco ISE machine account from the Active Directory database, the Active Directory credentials
that you provide here must have the permission to remove machine account from domain.

**Step 5** If you do not have the Active Directory credentials, check the No Credentials Available checkbox, and click OK.

If you check the Leave domain without credentials checkbox, the primary Cisco ISE node leaves the Active Directory
domain. The Active Directory administrator must manually remove the machine account that was created in Active
Directory during the time of the join.

---

**Configure Authentication Domains**

The domain to which Cisco ISE is joined to has visibility to other domains with which it has a trust relationship.
By default, Cisco ISE is set to permit authentication against all those trusted domains. You can restrict
interaction with the Active Directory deployment to a subset of authentication domains. Configuring
authentication domains enables you to select specific domains for each join point so that the authentications
are performed against the selected domains only. Authentication domains improve security because they
instruct Cisco ISE to authenticate users only from selected domains and not from all domains trusted from
join point. Authentication domains also improve performance and latency of authentication request processing
because authentication domains limit the search area (that is, where accounts matching to incoming username
or identity will be searched). It is especially important when incoming username or identity does not contain
domain markup (prefix or suffix). Due to these reasons, configuring authentication domains is a best practice,
and we highly recommended it.

**Step 1** Choose Administration > Identity Management > External Identity Sources > Active Directory.

**Step 2** Click the Authentication Domains tab.

A table appears with a list of your trusted domains. By default, Cisco ISE permits authentication against all trusted
domains.

**Step 3** To allow only specified domains, uncheck Use all Active Directory domains for authentication check box.
Step 4 Check the check box next to the domains for which you want to allow authentication, and click **Enable Selected**. In the **Authenticate** column, the status of this domain changes to Yes.

You can also disable selected domains.

Step 5 Click **Show Unusable Domains** to view a list of domains that cannot be used. Unusable domains are domains that Cisco ISE cannot use for authentication due to reasons such as one-way trust, selective authentication and so on.

**What to do next**

Configure Active Directory user groups.

**Configure Active Directory User Groups**

You must configure Active Directory user groups for them to be available for use in authorization policies. Internally, Cisco ISE uses security identifiers (SIDs) to help resolve group name ambiguity issues and to enhance group mappings. SID provides accurate group assignment matching.

**Step 1** Choose **Administration > Identity Management > External Identity Sources > Active Directory**.

**Step 2** Click the **Groups** tab.

**Step 3** Do one of the following:

a) Choose **Add > Select Groups From Directory** to choose an existing group.

b) Choose **Add > Add Group** to manually add a group. You can either provide both group name and SID or provide only the group name and press **Fetch SID**.

Do not use double quotes (") in the group name for the user interface login.

**Step 4** If you are manually selecting a group, you can search for them using a filter. For example, enter `admin*` as the filter criteria and click **Retrieve Groups** to view user groups that begin with admin. You can also enter the asterisk (*) wildcard character to filter the results. You can retrieve only 500 groups at a time.

**Step 5** Check the check boxes next to the groups that you want to be available for use in authorization policies and click **OK**.

**Step 6** If you choose to manually add a group, enter a name and SID for the new group.

**Step 7** Click **OK**.

**Step 8** Click **Save**.

**Note** If you delete a group and create a new group with the same name as original, you must click **Update SID Values** to assign new SID to the newly created group. After an upgrade, the SIDs are automatically updated after the first join.

**What to do next**

Configure Active Directory user attributes.

**Configure Active Directory User and Machine Attributes**

You must configure Active Directory user and machine attributes to be able to use them in conditions in authorization policies.
Modify Password Changes, Machine Authentications, and Machine Access Restriction Settings

Before you begin
You must join Cisco ISE to the Active Directory domain. For more information, see Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point, on page 329.

Step 1 Choose Administration > Identity Management > External Identity Sources > Active Directory.
Step 2 Check the check box next to the relevant Cisco ISE node and click Edit.
Step 3 Click the Advanced Settings tab.
Step 4 Modify as required, the Password Change, Machine Authentication, and Machine Access Restrictions (MARs) settings. These options are enabled by default.
Step 5 Check the Enable dial-in check box to check the dial-in permissions of the user during authentication or query. The result of the check can cause a reject of the authentication in case the dial-in permission is denied.
Step 6 Check the Enable callback check for dial-in clients check box if you want the server to call back the user during authentication or query. The IP address or phone number used by the server can be set either by the caller or the network administrator. The result of the check is returned to the device on the RADIUS response.
Step 7 Check the Use Kerberos for Plain Text Authentications check box if you want to use Kerberos for plain-text authentications. The default and recommended option is MS-RPC. Kerberos is used in ISE 1.2.
Machine Access Restriction (MAR) Cache Persistency

Cisco ISE stores the MAR cache content, calling-station-ID list, and the corresponding time stamps to a file on its local disk when you manually stop the Cisco ISE application services. Cisco ISE does not store the MAR cache entries of an instance when there is an accidental restart of its application services.

Cisco ISE reads the MAR cache entries from the file on its local disk based on the cache entry time to live when the Cisco ISE application services get restarted. When the application services of a Cisco ISE instance come up after a restart, Cisco ISE compares the current time of that instance with the MAR cache entry time. If the difference between the current time and the MAR entry time is greater than the MAR cache entry time to live, then Cisco ISE does not retrieve that entry from disk. Otherwise, Cisco ISE retrieves that MAR cache entry and updates its MAR cache entry time to live.

Configure Custom Schema

Before you begin

You must join Cisco ISE to the Active Directory domain.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; Identity Management &gt; External Identity Sources &gt; Active Directory.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select the Join point.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Advanced Settings tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Under the Schema section, select the Custom option from the Schema drop-down list. You can update the user information attributes based on your requirements. These attributes are used to collect user information, such as, first name, last name, email, telephone, locality, and so on. Predefined attributes are used for the Active Directory schema (built-in schema). If you edit the attributes of the predefined schema, Cisco ISE automatically creates a custom schema.</td>
</tr>
</tbody>
</table>

Support for Active Directory Multi-Join Configuration

Cisco ISE supports multiple joins to Active Directory domains. Cisco ISE supports up to 50 Active Directory joins. Cisco ISE can connect with multiple Active Directory domains that do not have a two-way trust or have zero trust between them. Active Directory multi-domain join comprises a set of distinct Active Directory domains with their own groups, attributes, and authorization policies for each join.

You can join the same forest more than once, that is, you can join more than one domain in the same forest, if necessary.

Cisco ISE now allows to join domains with one-way trust. This option helps bypass the permission issues caused by a one-way trust. You can join either of the trusted domains and hence be able to see both domains.

- **Join Point**—In Cisco ISE, each independent join to an Active Directory domain is called a join point. The Active Directory join point is an Cisco ISE identity store and can be used in authentication policy. It has an associated dictionary for attributes and groups, which can be used in authorization conditions.

- **Scope**—A subset of Active Directory join points grouped together is called a scope. You can use scopes in authentication policy in place of a single join point and as authentication results. Scopes are used to authenticate users against multiple join points. Instead of having multiple rules for each join point, if you use a scope, you can create the same policy with a single rule and save the time that Cisco ISE takes to
process a request and help improve performance. A join point can be present in multiple scopes. A scope can be included in an identity source sequence. You cannot use scopes in an authorization policy condition because scopes do not have any associated dictionaries.

When you perform a fresh Cisco ISE install, by default no scopes exist. This is called the no scope mode. When you add a scope, Cisco ISE enters multi-scope mode. If you want, you can return to no scope mode. All the join points will be moved to the Active Directory folder.

- Initial_Scope is an implicit scope that is used to store the Active Directory join points that were added in no scope mode. When multi-scope mode is enabled, all the Active Directory join points move into the automatically created Initial_Scope. You can rename the Initial_Scope.
- All_AD_Instances is a built-in pseudo scope that is not shown in the Active Directory configuration. It is only visible as an authentication result in policy and identity sequences. You can select this scope if you want to select all Active Directory join points configured in Cisco ISE.

Create a New Scope to Add Active Directory Join Points

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Administration &gt; Identity Management &gt; External Identity Sources &gt; Active Directory.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Scope Mode. A default scope called Initial_Scope is created, and all the current join points are placed under this scope.</td>
</tr>
<tr>
<td>Step 3</td>
<td>To create more scopes, click Add.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter a name and a description for the new scope.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Submit.</td>
</tr>
</tbody>
</table>

Identity Rewrite

Identity rewrite is an advanced feature that directs Cisco ISE to manipulate the identity before it is passed to the external Active Directory system. You can create rules to change the identity to a desired format that includes or excludes a domain prefix and/or suffix or other additional markup of your choice.

Identity rewrite rules are applied on the username or hostname received from the client, before being passed to Active Directory, for operations such as subject searches, authentication, and authorization queries. Cisco ISE will match the condition tokens and when the first one matches, Cisco ISE stops processing the policy and rewrites the identity string according to the result.

During the rewrite, everything enclosed in square bracket [ ] (such as [IDENTITY]) is a variable that is not evaluated on the evaluation side but instead added with the string that matches that location in the string. Everything without the brackets is evaluated as a fixed string on both the evaluation side and the rewrite side of the rule.

The following are some examples of identity rewrite, considering that the identity entered by the user is ACME\jdoe:

- If the identity matches ACME\[IDENTITY], rewrite as [IDENTITY].
  The result would be jdoe. This rule instructs Cisco ISE to strip all usernames with the ACME prefix.
- If the identity matches ACME\[IDENTITY], rewrite as [IDENTITY]@ACME.com.
The result would be jdoe@ACME.com. This rule instructs Cisco ISE to change the format from prefix for suffix notation or from NetBIOS format to UPN formats.

- If the identity matches **ACME\[IDENTITY\]**, rewrite as **ACME2\[IDENTITY\]**.
  The result would be ACME2\jdoe. This rule instructs Cisco ISE to change all usernames with a certain prefix to an alternate prefix.

- If the identity matches **[ACME]\jdoe.USA**, rewrite as **[IDENTITY]\@[ACME].com**.
  The result would be jdoe\ACME.com. This rule instructs Cisco ISE to strip the realm after the dot, in this case the country and replace it with the correct domain.

- If the identity matches **E=\[IDENTITY\]**, rewrite as **\[IDENTITY\]**.
  The result would be jdoe. This is an example rule that can be created when an identity is from a certificate, the field is an email address, and Active Directory is configured to search by Subject. This rule instructs Cisco ISE to remove ‘E=’.

- If the identity matches **E=[EMAIL],[DN]**, rewrite as **[DN]**.
  This rule will convert certificate subject from E=jdoe@acme.com, CN=jdoe, DC=acme, DC=com to pure DN, CN=jdoe, DC=acme, DC=com. This is an example rule that can be created when identity is taken from a certificate subject and Active Directory is configured to search user by DN. This rule instructs Cisco ISE to strip email prefix and generate DN.

The following are some common mistakes while writing the identity rewrite rules:

- If the identity matches **[DOMAIN]\[IDENTITY\]**, rewrite as **[IDENTITY]\@\[DOMAIN\].com**.
  The result would be jdoe@DOMAIN.com. This rule does not have [DOMAIN] in square brackets [ ] on the rewrite side of the rule.

- If the identity matches **DOMAIN\[IDENTITY\]**, rewrite as **[IDENTITY]\@\[DOMAIN\].com**.
  Here again, the result would be jdoe@DOMAIN.com. This rule does not have [DOMAIN] in square brackets [ ] on the evaluation side of the rule.

Identity rewrite rules are always applied within the context of an Active Directory join point. Even if a scope is selected as the result of an authentication policy, the rewrite rules are applied for each Active Directory join point. These rewrite rules also apply for identities taken from certificates if EAP-TLS is being used.

---

**Enable Identity Rewrite**

**Note**
This configuration task is optional. You can perform it to reduce authentication failures that can arise because of various reasons such as ambiguous identity errors.

**Before you begin**
You must join Cisco ISE to the Active Directory domain.

**Step 1**
Choose Administration > Identity Management > External Identity Sources > Active Directory.

**Step 2**
Click the Advanced Settings tab.
Step 3 Under the **Identity Rewrite** section, choose whether you want to apply the rewrite rules to modify usernames.

Step 4 Enter the match conditions and the rewrite results. You can remove the default rule that appears and enter the rule according to your requirement. Cisco ISE processes the policy in order, and the first condition that matches the request username is applied. You can use the matching tokens (text contained in square brackets) to transfer elements of the original username to the result. If none of the rules match, the identity name remains unchanged. You can click the **Launch Test** button to preview the rewrite processing.

---

**Identity Resolution Settings**

Some type of identities include a domain markup, such as a prefix or a suffix. For example, in a NetBIOS identity such as ACME\jdoe, “ACME” is the domain markup prefix, similarly in a UPN identity such as jdoe@acme.com, “acme.com” is the domain markup suffix. Domain prefix should match to the NetBIOS (NTLM) name of the Active Directory domain in your organization and domain suffix should match to the DNS name of Active Directory domain or to the alternative UPN suffix in your organization. For example jdoe@gmail.com is treated as without domain markup because gmail.com is not a DNS name of Active Directory domain.

The identity resolution settings allows you to configure important settings to tune the security and performance balance to match your Active Directory deployment. You can use these settings to tune authentications for usernames and hostnames without domain markup. In cases when Cisco ISE is not aware of the user's domain, it can be configured to search the user in all the authentication domains. Even if the user is found in one domain, Cisco ISE will wait for all responses in order to ensure that there is no identity ambiguity. This might be a lengthy process, subject to the number of domains, latency in the network, load, and so on.

**Avoid Identity Resolution Issues**

It is highly recommended to use fully qualified names (that is, names with domain markup) for users and hosts during authentication. For example, UPNs and NetBIOS names for users and FQDN SPNs for hosts. This is especially important if you hit ambiguity errors frequently, such as, several Active Directory accounts match to the incoming username; for example, jdoe matches to jdoe@emea.acme.com and jdoe@amer.acme.com. In some cases, using fully qualified names is the only way to resolve issue. In others, it may be sufficient to guarantee that the users have unique passwords. So, it is more efficient and leads to less password lockout issues if unique identities are used initially.

**Configure Identity Resolution Settings**

**Note**

This configuration task is optional. You can perform it to reduce authentication failures that can arise because of various reasons such as ambiguous identity errors.

**Before you begin**

You must join Cisco ISE to the Active Directory domain.

**Step 1** Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.

**Step 2** Click the **Advanced Settings** tab.
Step 3 Define the following settings for identity resolution for usernames or machine names under the **Identity Resolution** section. This setting provides you advanced control for user search and authentication.

The first setting is for the identities without a markup. In such cases, you can select any of the following options:

- **Reject the request**—This option will fail the authentication for users who do not have any domain markups, such as a SAM name. This is useful in case of multi join domains where Cisco ISE will have to look up for the identity in all the joined global catalogs, which might not be very secure. This option forces the users to use names with domain markups.
- **Only search in the “Authentication Domains” from the joined forest**—This option will search for the identity only in the domains in the forest of the join point which are specified in the authentication domains section. This is the default option and identical to Cisco ISE 1.2 behavior for SAM account names.
- **Search in all the “Authentication Domains” sections**—This option will search for the identity in all authentication domains in all the trusted forests. This might increase latency and impact performance.

The selection is made based on how the authentication domains are configured in Cisco ISE. If only specific authentication domains are selected, only those domains will be searched (for both “joined forest” or “all forests” selections).

The second setting is used if Cisco ISE cannot communicate with all Global Catalogs (GCs) that it needs to in order to comply with the configuration specified in the “Authentication Domains” section. In such cases, you can select any of the following options:

- **Proceed with available domains**—This option will proceed with the authentication if it finds a match in any of the available domains.
- **Drop the request**—This option will drop the authentication request if the identity resolution encounters some unreachable or unavailable domain.

---

**Test Users for Active Directory Authentication**

The Test User tool can be used to verify user authentication from Active Directory. You can also fetch groups and attributes and examine them. You can run the test for a single join point or for scopes.

**Step 1** Choose **Administration > Identity Management > External Identity Sources > Active Directory**.

**Step 2** Choose one of the following options:

- To run the test on all join points, choose **Advanced Tools > Test User for All Join Points**.
- To run the test for a specific join point, select the joint point and click **Edit**. Select the Cisco ISE node and click **Test User**.

**Step 3** Enter the username and password of the user (or host) in Active Directory.

**Step 4** Choose the authentication type. Password entry in step 3 is not required if you choose the Lookup option.

**Step 5** Select the Cisco ISE node on which you want to run this test, if you are running this test for all join points.

**Step 6** Check the Retrieve Groups and Attributes checkboxes if you want to retrieve the groups and attributes from Active Directory.

**Step 7** Click **Test**. The result and steps of the test operation are displayed. The steps can help to identify the failure reason and troubleshoot.
You can also view the time taken (in milliseconds) for Active Directory to perform each processing step (for authentication, lookup, or fetching groups/attributes). Cisco ISE displays a warning message if the time taken for an operation exceeds the threshold.

## Delete Active Directory Configurations

You should delete Active Directory configurations if you are not going to use Active Directory as an external identity source. Do not delete the configuration if you want to join another Active Directory domain. You can leave the domain to which you are currently joined and join a new domain.

### Before you begin

Ensure that you have left the Active Directory domain.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Administration</strong> &gt; <strong>Identity Management</strong> &gt; <strong>External Identity Sources</strong> &gt; <strong>Active Directory</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Check the checkbox next to the configured Active Directory.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Check and ensure that the Local Node status is listed as Not Joined.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Delete</strong>.</td>
</tr>
</tbody>
</table>

You have removed the configuration from the Active Directory database. If you want to use Active Directory at a later point in time, you can resubmit a valid Active Directory configuration.

## View Active Directory Joins for a Node

You can use the **Node View** button on the **Active Directory** page to view the status of all Active Directory join points for a given Cisco ISE node or a list of all join points on all Cisco ISE nodes.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Administration</strong> &gt; <strong>Identity Management</strong> &gt; <strong>External Identity Sources</strong> &gt; <strong>Active Directory</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click <strong>Node View</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select a node from the <strong>ISE Node</strong> drop-down list. The table lists the status of Active Directory by node. If there are multiple join points and multiple Cisco ISE nodes in a deployment, this table may take several minutes to update.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click the join point <strong>Name</strong> link to go to that Active Directory join point page and perform other specific actions.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click the link in the <strong>Diagnostic Summary</strong> column to go to the <strong>Diagnostic Tools</strong> page to troubleshoot specific issues. The diagnostic tool displays the latest diagnostics results for each join point per node.</td>
</tr>
</tbody>
</table>

## Diagnose Active Directory Problems

The Diagnostic Tool is a service that runs on every Cisco ISE node. It allows you to automatically test and diagnose the Active Directory deployment and execute a set of tests to detect issues that may cause functionality or performance failures when Cisco ISE uses Active Directory.
There are multiple reasons for which Cisco ISE might be unable to join or authenticate against Active Directory. This tool helps ensure that the prerequisites for connecting Cisco ISE to Active Directory are configured correctly. It helps detect problems with networking, firewall configurations, clock sync, user authentication, and so on. This tool works as a step-by-step guide and helps you fix problems with every layer in the middle, if needed.

**Step 1** Choose Administration > Identity Management > External Identity Sources > Active Directory.

**Step 2** Click the Advanced Tools drop-down and choose Diagnostic Tools.

**Step 3** Select a Cisco ISE node to run the diagnosis on.

If you do not select a Cisco ISE node then the test is run on all the nodes.

**Step 4** Select a specific Active Directory join point.

If you do not select an Active Directory join point then the test is run on all the join points.

**Step 5** Click Run All Tests on Node to start the test.

**Step 6** Click View Test Details to view the details for tests with Warning or Failed status.

This table allows you to rerun specific tests, stop running tests, and view a report of specific tests.

---

**Enable Active Directory Debug Logs**

Active Directory debug logs are not logged by default. You must enable this option on the Cisco ISE node that has assumed the Policy Service persona in your deployment. Enabling Active Directory debug logs may affect ISE performance.

**Step 1** Choose Administration > System > Logging > Debug Log Configuration.

**Step 2** Click the radio button next to the Cisco ISE Policy Service node from which you want to obtain Active Directory debug information, and click Edit.

**Step 3** Click the Active Directory radio button, and click Edit.

**Step 4** Choose DEBUG from the drop-down list next to Active Directory. This will include errors, warnings, and verbose logs. To get full logs, choose TRACE.

**Step 5** Click Save.

---

**Obtain the Active Directory Log File for Troubleshooting**

Download and view the Active Directory debug logs to troubleshoot issues you may have.

**Before you begin**

Active Directory debug logging must be enabled.

**Step 1** Choose Operations > Troubleshoot > Download Logs.

**Step 2** Click the node from which you want to obtain the Active Directory debug log file.
Active Directory Alarms and Reports

Cisco ISE provides various alarms and reports to monitor and troubleshoot Active Directory related activities.

Alarms

The following alarms are triggered for Active Directory errors and issues:

- Configured nameserver not available
- Joined domain is unavailable
- Authentication domain is unavailable
- Active Directory forest is unavailable
- AD Connector had to be restarted
- AD: ISE account password update failed
- AD: Machine TGT refresh failed

Reports

You can monitor Active Directory related activities through the following two reports:

- RADIUS Authentications Report—This report shows detailed steps of the Active Directory authentication and authorization. You can find this report here: Operations > Reports > Auth Services Status > RADIUS Authentications.

- AD Connector Operations Report—The AD Connector Operations report provides a log of background operations performed by AD connector, such as Cisco ISE server password refresh, Kerberos ticket management, DNS queries, DC discovery, LDAP, and RPC connections management. If you encounter any Active Directory failures, you can review the details in this report to identify the possible causes. You can find this report here: Operations > Reports > Auth Services Status > AD Connector Operations.

Active Directory Advanced Tuning

The advanced tuning feature provides node-specific settings used for support action under the supervision of Cisco support personnel, to adjust the parameters deeper in the system. These settings are not intended for normal administration flow, and should be used only under guidance.

Active Directory Identity Search Attributes

Cisco ISE identifies users using the attributes SAM, CN, or both. Cisco ISE, Release 2.2 Patch 5 and above, and 2.3 Patch 2 and above, use sAMAccountName attribute as the default attribute. In earlier releases, both SAM and CN attributes were searched by default. This behavior has changed in Release 2.2 Patch 5 and
above, and 2.3 Patch 2 and above, as part of CSCvF21978 bug fix. In these releases, only the sAMAccountName attribute is used as the default attribute.

You can configure Cisco ISE to use SAM, CN, or both, if your environment requires it. When SAM and CN are used, and the value of the SAMAccountName attribute is not unique, Cisco ISE also compares the CN attribute value.

**Configure Attributes for Active Directory Identity Search**

1. Choose Administration > Identity Management > External Identity Sources > Active Directory. In the Active Directory window, click Advanced Tools, and choose Advanced Tuning. Enter the following details:
   - **ISE Node**—Choose the ISE node that is connecting to Active Directory.
   - **Name**—Enter the registry key that you are changing. To change the Active Directory search attributes, enter: REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\IdentityLookupField
   - **Value**—Enter the attributes that ISE uses to identify a user:
     - **SAM**—To use only SAM in the query (this option is the default).
     - **CN**—To use only CN in the query.
     - **SAMCN**—To use CN and SAM in the query.
   - **Comment**—Describe what you are changing, for example: Changing the default behavior to SAM and CN

2. Click Update Value to update the registry.
   A pop-up window appears. Read the message and accept the change. The AD connector service in ISE restarts.

**Example Search Strings**

For the following examples, assume that the username is *userd2only*:

- **SAM search string**—
  filter={(|(objectCategory=person) (objectCategory=computer)) ((cn=userd2only) (sAMAccountName=userd2only))}

- **SAM and CN search string**—
  filter={(|(objectCategory=person) (objectCategory=computer)) (sAMAccountName=userd2only)}

---

**Supplemental Information for Setting Up Cisco ISE with Active Directory**

For configuring Cisco ISE with Active Directory, you must configure group policies, and configure a supplicant for machine authentication.

**Configure Group Policies in Active Directory**

For more information about how to access the Group Policy management editor, refer to the Microsoft Active Directory documentation.
Configure Odyssey 5.X Supplicant for EAP-TLS Machine Authentications Against Active Directory

If you are using the Odyssey 5.x supplicant for EAP-TLS machine authentications against Active Directory, you must configure the following in the supplicant.
**Step 1** Start Odyssey Access Client.

**Step 2** Choose Odyssey Access Client Administrator from the Tools menu.

**Step 3** Double-click the Machine Account icon.

**Step 4** From the Machine Account page, you must configure a profile for EAP-TLS authentications:

a) Choose Configuration > Profiles.

b) Enter a name for the EAP-TLS profile.

c) On the Authentication tab, choose EAP-TLS as the authentication method.

d) On the Certificate tab, check the Permit login using my certificate check box, and choose a certificate for the supplicant machine.

e) On the User Info tab, check the Use machine credentials check box.

If this option is enabled, the Odyssey supplicant sends the machine name in the format host\<machine_name> and Active Directory identifies the request as coming from a machine and will look up computer objects to perform authentication. If this option is disabled, the Odyssey supplicant sends the machine name without the host\ prefix and Active Directory will look up user objects and the authentication fails.

---

**AnyConnect Agent for Machine Authentication**

When you configure AnyConnect Agent for machine authentication, you can do one of the following:

- Use the default machine hostname, which includes the prefix “host/.”

- Configure a new profile, in which case you must include the prefix “host/” and then the machine name.

---

**Active Directory Requirements to Support Easy Connect and Passive Identity services**

Easy Connect and Passive Identity services use Active Directory login audit events generated by the Active Directory domain controller to gather user login information. The Active Directory server must be configured properly so the ISE user can connect and fetch the user login information. The following sections show how configure the Active Directory domain controller (configurations from the Active Directory side) to support Easy Connect and Passive Identity services.

In order to configure Active Directory domain controllers (configurations from the Active Directory side) to support Easy Connect and Passive Identity services use, follow these steps:

1. Set up Active Directory join points and domain controllers from ISE. See Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point, on page 329 and Add Domain Controllers, on page 331.

2. Configure WMI per domain controller. See Configure WMI, on page 331.

3. Perform the following steps from Active Directory:
   
   - Configure Active Directory for Passive Identity service, on page 346
   - Set the Windows Audit Policy, on page 349
Configure Active Directory for Passive Identity service

ISE Easy Connect and Passive Identity services use Active Directory login audit events generated by the Active Directory domain controller to gather user login information. ISE connects to Active Directory and fetches the user login information.

The following steps should be performed from the Active Directory domain controller:

**Step 1**  
Make sure relevant Microsoft patches are installed on the Active Directory domain controllers.

a) The following patches for Windows Server 2008 are required:

- [http://support.microsoft.com/kb/958124](http://support.microsoft.com/kb/958124)
  
  This patch fixes a memory leak in Microsoft’s WMI, which prevents ISE to establish successful connection with the domain controller (ISE administrator can experience it in ISE Active Directory domain controller GUI page, where the status need to be “up” once the connection establishes successfully).

- [http://support.microsoft.com/kb/973995](http://support.microsoft.com/kb/973995)
  
  This patch fixes different memory leak in Microsoft’s WMI, which sporadically prevents the Active Directory domain controller from writing the necessary user login events to the Security Log of the domain controller. As result ISE may not get all user login events from this domain controller.

b) The following patches for Windows Server 2008 R2 are required (unless SP1 is installed):

- [http://support.microsoft.com/kb/981314](http://support.microsoft.com/kb/981314)
  
  This patch fixes memory leak in Microsoft’s WMI, which sporadically prevents the Active Directory domain controller from writing the necessary user login events to the Security Log of the domain controller. As result ISE may not get all user login events from this domain controller.

- [http://support.microsoft.com/kb/2617858](http://support.microsoft.com/kb/2617858)
  
  This patch fixes unexpectedly slow startup or logon process in Windows Server 2008 R2.

c) The patches listed at the following link, for WMI related issues on Windows platform are required:

- [http://support.microsoft.com/kb/2591403](http://support.microsoft.com/kb/2591403)

  These hot fixes are associated with the operation and functionality of the WMI service and its related components.

**Step 2** Make sure the Active Directory logs the user login events in the Windows Security Log.
Verify that the settings of the “Audit Policy” (part of the “Group Policy Management” settings) allows successful logons to generate the necessary events in the Windows Security Log (this is the default Windows setting, but you must explicitly ensure that this setting is correct). See Setting the Windows Audit Policy.

**Step 3**

You must have an Active Directory user with sufficient permissions for ISE to connect to the Active Directory. The following instructions show how to define permissions either for admin domain group user or none admin domain group user:

- Permissions Required when an Active Directory User is a Member of the Domain Admin Group, page 2-4
- Permissions Required when an Active Directory User is Not a Member of the Domain Admin Group, page 2-4

**Step 4**

The Active Directory user used by ISE can be authenticated either by NT Lan Manager (NTLM) v1 or v2. You need to verify that the Active Directory NTLM settings are aligned with ISE NTLM settings to ensure successful authenticated connection between ISE and the Active Directory Domain Controller. The following table shows all Microsoft NTLM options, and which ISE NTLM actions are supported. If ISE is set to NTLMv2, all six options described in are supported. If ISE is set to support NTLMv1, only the first five options are supported.

<table>
<thead>
<tr>
<th>ISE NTLM setting options / Active Directory (AD) NTLM setting options</th>
<th>NTLMv1</th>
<th>NTLMv2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send LM &amp; NTLM responses. Connection is allowed.</td>
<td>connection is allowed</td>
<td>connection is allowed</td>
</tr>
<tr>
<td>Send LM &amp; NTLM - use NTLMv2 session security if negotiated. Connection is allowed.</td>
<td>connection is allowed</td>
<td>connection is allowed</td>
</tr>
<tr>
<td>Send NTLM response only. Connection is allowed.</td>
<td>connection is allowed</td>
<td>connection is allowed</td>
</tr>
<tr>
<td>Send NTLMv2 response only. Connection is allowed.</td>
<td>connection is allowed</td>
<td>connection is allowed</td>
</tr>
<tr>
<td>Send NTLMv2 response only. Refuse LM connection is allowed.</td>
<td>connection is allowed</td>
<td>connection is allowed</td>
</tr>
<tr>
<td>Send NTLMv2 response only. Refuse LM &amp; NTLM connection is refused.</td>
<td>connection is refused</td>
<td>connection is allowed</td>
</tr>
</tbody>
</table>
Step 5

Make sure that you have created a firewall rule to allow traffic to dllhost.exe on Active Directory domain controllers. You can either turn the firewall off, or allow access on a specific IP (ISE IP address) to the following ports:

- **TCP 135**: General RPC Port. When doing asynchronous RPC calls, the service listening on this port tells the client which port the component servicing this request is using.
- **UDP 137**: Netbios Name Resolution
- **UDP 138**: Netbios Datagram Service
- **TCP 139**: Netbios Session Service
- **TCP 445**: SMB

Higher ports are assigned dynamically or you can configure them manually. We recommend that you add %SystemRoot%\System32\dllhost.exe as a target. This program manages ports dynamically.

All firewall rules can be assigned to specific IP (ISE IP).
Set the Windows Audit Policy

Ensure that the Audit Policy (part of the Group Policy Management settings) allows successful logons. This is required to generate the necessary events in the Windows Security Log of the AD domain controller machine. This is the default Windows setting, but you must verify that this setting is correct.

Step 1  Choose Start > Programs > Administrative Tools > Group Policy Management.

Step 2  Navigate under Domains to the relevant domain and expand the navigation tree.

Step 3  Choose Default Domain Controller Policy, right click and choose Edit.

The Group Policy Management Editor appears.


- For Windows Server 2003 or Windows Server 2008 (non-R2), choose Local Policies > Audit Policy. For the two Policy items, Audit Account Logon Events and Audit Logon Events, ensure that the corresponding Policy Setting either directly or indirectly includes the Success condition. To include the Success condition indirectly, the Policy Setting must be set to Not Defined, indicating that the effective value will be inherited from a higher level domain, and the Policy Setting for that higher level domain must be configured to explicitly include the Success condition.

- For Windows Server 2008 R2 and Windows 2012, choose Advanced Audit Policy Configuration > Audit Policies > Account Logon. For the two Policy items, Audit Kerberos Authentication Service and Audit Kerberos Service Ticket Operations, ensure that the corresponding Policy Setting either directly or indirectly includes the Success condition, as described above.

Step 5  If any Audit Policy item settings have been changed, you should then run gpupdate /force to force the new settings to take effect.

Set Permissions When AD User in the Domain Admin Group

For Windows 2008 R2, Windows 2012, and Windows 2012 R2, the Domain Admin group does not have full control on certain registry keys in the Windows operating system by default. The Active Directory admin must give the Active Directory user Full Control permissions on the following registry keys:

- HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
- HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

No registry changes are required for the following Active Directory versions:

- Windows 2003
- Windows 2003R2
- Windows 2008

To grant full control, the Active Directory admin must first take ownership of the key, as shown below.

Step 1  Go to the Owner tab by right clicking the key.
Step 2  Click Permissions.
Step 3  Click Advanced.

Required Permissions when AD User not in Domain Admin Group

For Windows 2012 R2, give the Active Directory user Full Control permissions on the following registry keys:

- HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}
- HKLM\Software\Classes\Wow6432Node\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}

The following permissions also are required when an Active Directory user is not in the Domain Admin group, but is in the Domain Users group:

- Add Registry Keys to Allow ISE to Connect to the Domain Controller (see below)
- Permissions to Use DCOM on the Domain Controller, on page 249
- Set Permissions for Access to WMI Root/CIMv2 Name Space, on page 251

These permissions are only required for the following Active Directory versions:

- Windows 2003
- Windows 2003R2
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

Add Registry Keys to Allow ISE to Connect to the Domain Controller

You must manually add some registry keys to the domain controller to allow ISE to connect as a Domain User, and retrieve login authentication events. An agent is not required on the domain controllers or on any machine in the domain.

The following registry script shows the keys to add. You can copy and paste this into a text file, save the file with a .reg extension, and double click the file to make the registry changes. To add registry keys, the user must be an owner of the root group.

Windows Registry Editor Version 5.00

[HKEY_CLASSES_ROOT\CLSID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"AppID"="{76A64158-CB41-11D1-8B02-00600806D9B6}"

[HKEY_CLASSES_ROOT\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]
"DllSurrogate"=""

[HKEY_CLASSES_ROOT\Wow6432Node\AppID\{76A64158-CB41-11D1-8B02-00600806D9B6}]

"DllSurrogate"=" "

Make sure that you include two spaces in the value of the key DllSurrogate.
Keep the empty lines as shown in the script above, including an empty line at the end of the file.

Permissions to Use DCOM on the Domain Controller

The Active Directory user used for ISE Passive Identity services must have permissions to use DCOM (remote COM) on the Domain Controller. You can configure permissions with the dcomcnfg command line tool.

Step 1 Run the dcomcnfg tool from the command line.
Step 2 Expand Component Services.
Step 3 Expand Computers > My Computer.
Step 4 Select Action from the menu bar, click properties, and click COM Security.
Step 5 Make sure that the account that ISE will use for both Access and Launch has Allow permissions. That Active Directory user should be added to all the four options (Edit Limits and Edit Default for both Access Permissions and Launch and Activation Permissions).
Step 6 Allow all Local and Remote access for both Access Permissions and Launch and Activation Permissions.

Figure 23: Local and Remote Access for Access Permissions
Set Permissions for Access to WMI Root/CIMv2 Name Space

By default, Active Directory users do not have permissions for the Execute Methods and Remote Enable. You can grant access using the wmiimgt.msc MMC console.

Step 1  Click Start > Run and type wmiimgt.msc.
Step 2  Right-click WMI Control and click Properties.
Step 3  Under the Security tab, expand Root and choose CIMV2.
Step 4  Click Security.
Step 5  Add the Active Directory user, and configure the required permissions as shown below.
Grant Access to the Security Event Log on the AD Domain Controller

On Windows 2008 and later, you can grant access to the AD Domain controller logs by adding the ISE ID Mapping user to a group called Event Log Readers.

On all older versions of Windows, you must edit a registry key, as shown below.

**Step 1**
To delegate access to the Security event logs, find the SID for the account.

**Step 2**
Use the following command from the command line, also shown in the diagram below, to list all the SID accounts.

```
wmic useraccount get name,sid
```

You can also use the following command for a specific username and domain:

```
wmic useraccount where name="iseUser" get domain,name,sid
```
Step 3  Find the SID, open the Registry Editor, and browse to the following location:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog

Step 4  Click on Security, and double click CustomSD. See Figure 2-7

For example, to allow read access to the ise_agent account (SID = S-1-5-21-1742827456-3351963980-3809373604-1107), enter (A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107).

Step 5  Restart the WMI service on the Domain Controller. You can restart the WMI services in the following two ways:

a)  Run the following commands from the CLI:

   net stop winmgmt

   net start winmgmt

b)  Run Services.msc, which opens the Windows Services Management tool. In the Windows Services Management window, locate the Windows Management Instrumentation service, right click, and select Restart.
**Easy Connect**

Easy Connect enables you to easily connect users from a wired endpoint to a network in a secure manner and monitor those users by authenticating them through an Active Directory Domain Controller and not by Cisco ISE. With Easy Connect, ISE collects user authentication information from the Active Directory Domain Controller. Because Easy Connect connects to a Windows system (Active Directory) using the MS WMI interface and queries logs from the Windows event messaging, it currently only supports Windows-installed endpoints. Easy Connect supports wired connections using MAB, which is much easier to configure than 802.1X. Unlike 802.1X, with Easy Connect and MAB:

- You don't need to configure supplicants
- You don't need to configure PKI
- ISE issues a CoA after the external server (AD) authenticates the user

Easy Connect supports these modes of operation:

- Enforcement-mode—ISE actively downloads the authorization policy to the network device for enforcement based on the user credentials.
  - Visibility-mode—ISE publishes session merge and accounting information received from the NAD device sensor in order to send that information to pxGrid.

In both cases, users authenticated with Active Directory (AD) are shown in the Cisco ISE live sessions view, and can be queried from the session directory using Cisco pxGrid interface by third-party applications. The known information is the user name, IP address, the AD DC host name and the AD DC NetBios name. For more information about pxGrid, see pxGrid Node, on page 64.

Once you have set up Easy Connect, you can then filter certain users, based on their name or IP address. For example, if you have an administrator from IT services who logs in to an endpoint in order to assist the regular user with that endpoint, you can filter out the administrator activity so it does not appear in Live Sessions, but rather only the regular user of that endpoint will appear. To filter passive identity services, see Filter Passive Identity Services, on page 402.

**Easy Connect Restrictions**

- MAC Authentication Bypass (MAB) supports Easy Connect. Both MAB and 802.1X can be configured on the same port, but you must have a different ISE policy for each service.
- Only MAB connections are currently supported. You do not need a unique authentication policy for connections, because the connection is authorized and permissions are granted by an Easy Connect condition defined in the authorization policy.
- Easy Connect is supported in High Availability mode. Multiple nodes can be defined and enabled with a Passive ID. ISE then automatically activates one PSN, while the other nodes remain in standby.
- Only Cisco Network Access Devices (NADs) are supported.
- IPv6 is not supported.
- Wireless connections are not currently supported.
- Only Kerberos auth events are tracked and therefore Easy Connect enables only user authentication and does not support machine authentication.
Easy Connect requires configuration in ISE, while the Active Directory Domain server must also have the correct patches and configuration based on instructions and guidelines issued by Microsoft. For information about configuring the Active Directory domain controller for ISE, see Active Directory Requirements to Support Easy Connect and Passive Identity services, on page 345.

**Easy Connect Enforcement Mode**

Easy Connect enables users to log on to a secure network from a wired endpoint (usually a PC) with a Windows operating system, by using MAC address bypass (MAB) protocol, and accessing Active Directory (AD) for authentication. ISE Easy Connect listens for a Windows Management Instrumentation (WMI) event from the Active Directory server for information about authenticated users. Once AD authenticates a user, the Domain Controller generates an event log that includes the user name and IP address allocated for the user. ISE receives notification of log in from AD, and then issues a RADIUS Change of Authorization (CoA).

---

**Note**

MAC address lookup is not done for a MAB request when the Radius service-type is set to call-check. Therefore the return to the request is access-accept. This is the ISE default configuration.

**Easy Connect Enforcement Mode Process Flow**

The Easy Connect Enforcement mode process is as follows:

1. The user connects to the NAD from a wired endpoint (such as a PC for example).
2. The NAD (which is configured for MAB) sends an access request to ISE. ISE responds with access, based on user configuration, allowing the user to access AD. Configuration must allow at least access to DNS, DHCP and AD.
3. The user logs in to the domain and a security audit event is sent to ISE.
4. ISE collects the MAC address from RADIUS and the IP address and domain name, as well as accounting information (login information) about the user, from the security audit event.
5. Once all data is collected and merged in the ISE session directory, ISE issues a CoA to the NAD (based on the appropriate policy managed in the policy service node (PSN)), and the user is provided access by the NAD to the network based on that policy.

*Figure 28: Easy Connect Enforcement Mode Basic Flow*
For more information about configuring Enforcement mode, see Configure Easy Connect Enforcement-Mode, on page 358.

**Easy Connect Visibility Mode**

With the Visibility mode, ISE only monitors accounting information from RADIUS (part of the device sensor feature in the NAD) and does not perform authorization. Easy Connect listens for RADIUS Accounting and WMI events, and publishes that information to logs and reports, (and optionally, to pxGrid). Both RADIUS accounting start and session termination are published to pxGrid during user login using Active Directory when pxGrid is setup.
Configure Easy Connect Enforcement-Mode

**Before you begin**

- For best performance, deploy a dedicated PSN to receive WMI events.
- Create a list of Active Directory Domain Controllers for the WMI node, which receives AD login events.
- Determine the Microsoft Domain that ISE must join to fetch user groups from Active Directory.
- Determine the Active Directory groups that are used as a reference in the authorization policy.
- If you are using pxGrid to share session data from network devices with other pxGrid-enabled systems, then define a pxGrid persona in your deployment. For more information about pxGrid, see pxGrid Node, on page 64.
- After successful MAB, the NAD must provide a limited-access profile, which allows the user on that port access to the Active Directory server (as described in the overview).

---

**Step 1**

**Note** Passive Identity Service can be enabled on multiple nodes, but Easy Connect can only operate on one node at a time. If you enable the service for multiple nodes, ISE will automatically determine which node to use for the active Easy Connect session.

Enable the Passive Identity service on the dedicated Policy server (PSN) you intend to use for Easy Connect, so ISE can get group information and event information from Active Directory — Choose **Administration > System > Deployment**, open a node, and under **General Settings**, enable **Enable Passive Identity Service**.

**Step 2**

Configure an Active Directory join point and domain controller to be used by Easy Connect. To do this, and for more information, see **Active Directory Requirements to Support Easy Connect and Passive Identity services**, on page 345.

**Step 3**

Optionally, map AD domain controller groups in order to create different policies for different groups of users (for example, a different policy for Marketing employees versus Administration employees) — Choose **Administration >**
Identity Management > External Identity Sources > Active Directory, select the Active Directory to use, select the Groups tab, and add the Active Directory groups you plan to use in your authorization policies. The Active Directory groups that you map for the Domain Controller are dynamically updated in the PassiveID dictionary and can then be used when you set up your policy conditions rules.

**Step 4**  
**Note**  
Passive Identity Tracking must be enabled for all profiles used for Easy Connect authorization in order for the Easy Connect process to run properly and enable ISE to issue a CoA.

Activate passive identity tracking—Choose Policy > Policy Elements > Results > Authorization > Authorization Profiles. For any profiles to be used by Easy Connect, open the profile and enable Passive Identify Tracking.

**Step 5**  
Create policy rules—Choose Policy > Policy Elements > Conditions > Authorization > Simple Conditions, to create rules for Easy Connect. Click Add. Then define the condition:

a) Enter a useful name and description.

b) From Attribute, go to the PassiveID dictionary and select either PassiveID_Groups to create a condition for domain controller groups, or select PassiveID_user to create a condition for individual users.

c) Enter the correct operation.

d) Enter the username or group name to be included in the policy.

**Step 6**  
Click Submit.

---

**Configure Easy Connect Visibility-Mode**

**Before you begin**

- For best performance, deploy a dedicated PSN to receive WMI events.
- Create a list of Active Directory Domain Controllers for the WMI node, which receives AD login events.
- Determine the Microsoft Domain that ISE must join to fetch user groups from Active Directory.
- If you are using pxGrid to share session data from network devices with other pxGrid-enabled systems, then define a pxGrid persona in your deployment. For more information about pxGrid, see pxGrid Node, on page 64

**Step 1**  
Enable the Passive Identity service on the dedicated Policy server (PSN) you intend to use for Easy Connect, so ISE can get group information and event information from Active Directory — Choose Administration > System > Deployment, open a node, and under General Settings, enable Enable Passive Identity Service.

**Step 2**  
Configure an Active Directory join point and domain controller to be used by Easy Connect. To do this, and for more information, see Active Directory Requirements to Support Easy Connect and Passive Identity services, on page 345.

---

**PassiveID Work Center**

Passive Identity Connector (the PassiveID work center) offers a centralized, one-stop installation and implementation enabling you to easily and simply configure your network in order to receive and share user identity information with a variety of different security product subscribers such as Cisco Firepower Management Center (FMC) and Stealthwatch. As the full broker for passive identification, the PassiveID
work center collects user identities from different provider sources, such as Active Directory Domain Controllers (AD DC), maps the user login information to the relevant IP addresses in use and then shares that mapping information with any of the subscriber security products that you have configured.

**What is Passive Identity?**

Standard flows offered by Cisco Identity Services Engine (ISE), which provide an authentication, authorization and accounting (AAA) server, and utilize technologies such as 802.1X or Web Authentication, communicate directly with the user or endpoint, requesting access to the network, and then using their login credentials in order to verify and actively authenticate their identity.

Passive identity services do not authenticate users directly, but rather gather user identities and IP addresses from external authentication servers such as Active Directory, known as providers, and then share that information with subscribers. The PassiveID work center first receives the user identity information from the provider, usually based on the user login and password, and then performs the necessary checks and services in order to match the user identity with the relevant IP address, thereby delivering the authenticated IP address to the subscriber.

**Passive Identity Connector (the PassiveID work center) Flow**

The flow for the PassiveID work center is as follows:

1. Provider performs the authentication of the user or endpoint.
2. Provider sends authenticated user information to .
3. ISE normalizes, performs lookups, merges, parses and maps user information to IP addresses and publishes mapped details to pxGrid.
4. pxGrid subscribers receive the mapped user details.

The following diagram illustrates the high-level flow offered by ISE.

**Figure 31: High Level Flow**

---

**Initial Setup and Configuration**

To get started using Cisco PassiveID work center quickly, follow this flow:
1. Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from ISE. For more information, see DNS Server, on page 328.

2. Enable the Passive Identity and pxGrid services on the dedicated Policy server (PSN) you intend to use for any of the Passive Identity services — Choose Administration > System > Deployment, open the relevant node, and under General Settings, enable Enable Passive Identity Service and pxGrid.

3. Synchronize clock settings for the NTP servers.

4. Configure an initial provider with the ISE Passive Identity Setup. For more information, see Getting Started with the Passive ID Setup, on page 362

5. Configure a single or multiple subscribers. For more information, see Subscribers, on page 405

After setting up an initial provider and subscriber, you can easily create additional providers (see Additional Passive Identity Service Providers, on page 368) and manage your passive identification from the different providers in the PassiveID work center:

- RADIUS Live Sessions, on page 1156
- Cisco ISE Alarms, on page 862
- Reports, on page 905
- TCP Dump Utility to Validate the Incoming Traffic, on page 892

PassiveID Work Center Dashboard

The Cisco PassiveID Work Center dashboard displays consolidated and correlated summary and statistical data that is essential for effective monitoring and troubleshooting, and is updated in real time. Dashlets show activity over the last 24 hours, unless otherwise noted. To access the dashboard, choose Work Centers > PassiveID and then from the left panel choose Dashboard. You can only view the Cisco PassiveID Work Center Dashboard in the Primary Administration Node (PAN).

The Home page has two default dashboards that show a view of your PassiveID Work Center data:

- **Main**—This view has a linear Metrics dashboard, chart dashlets, and list dashlets. In the PassiveID Work Center, the dashlets are not configurable. Available dashlets include:

  - **Passive Identity Metrics**—Passive Identity Metrics provides an overview of: the total number of unique live sessions currently being tracked, the total number of identity providers configured in the system, the total number of agents actively delivering identity data, and the total number of subscribers currently configured.

  - **Providers**—Providers provide user identity information to PassiveID Work Center. You configure the ISE probe (mechanisms that collect data from a given source) through which to receive information from the provider sources. For example, an Active Directory (AD) probe and an Agents probe both help ISE-PIC collect data from AD (each with different technology) while a Syslog probe collects data from a parser that reads syslog messages.

  - **Subscribers**—Subscribers connect to ISE to retrieve user identity information.

  - **OS Types**—The only OS type that can be displayed is Windows. Windows types display by Windows versions. Providers do not report the OS type, but ISE can query Active Directory to get that information. Up to 1000 entries are displayed in the dashlet. If you have more endpoints than that, or if you wish to display more OS types than Windows, you can upgrade to ISE.
Active Directory as a Probe and a Provider

Active Directory (AD) is a highly secure and precise source from which to receive user identity information, including user name, IP address and domain name.

The AD probe, a Passive Identity service, collects user identity information from AD through WMI technology, while other probes use AD as a user identity provider through other technologies and methods. For more information about other probes and provider types offered by ISE, see Additional Passive Identity Service Providers, on page 368.

By configuring the Active Directory probe you can also then quickly configure and enable these other probes (which also use Active Directory as their source):

- **Agent**—Active Directory Agents, on page 370

  ![Note](//)
  The Active Directory agents are only supported on Windows Server 2008 and higher.

- **SPAN**—SPAN, on page 379

- **Endpoint probe**—Endpoint Probe, on page 403

In addition, configure the Active Directory probe in order to use AD user groups when collecting user information. You can use AD user groups for the AD, Agents, SPAN and Syslog probes. For more information about AD groups, see Configure Active Directory User Groups, on page 333.

Set Up an Active Directory (WMI) Probe

To configure Active Directory and WMI for Passive Identity services you can use the Passive ID Work Center Wizard (see Getting Started with the PassiveID Setup, on page 362) or you can follow the steps as follows (and see Active Directory Requirements to Support Easy Connect and Passive Identity services, on page 345 for additional information):

1. Configure the Active Directory probe. See Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point, on page 329.

2. Create a list of Active Directory Domain Controllers for the WMI-configured node (or nodes) that receives AD login events. See Add Domain Controllers, on page 331.

3. Configure the Active Directory in order for it to integrate with ISE. See Configure WMI, on page 331.

4. (Optional) Manage the Active Directory Provider, on page 365.

Getting Started with the PassiveID Setup

ISE-PIC offers a wizard from which you can easily and quickly configure Active Directory as your first user identity provider, in order to receive user identities from Active Directory. By configuring Active Directory for ISE-PIC, you also simplify the process for configuring other provider types later on. Once you have configured Active Directory, you must then configure a Subscriber (such as Cisco Firepower Management...
Center (FMC) or Stealthwatch), in order to define the client that is to receive the user data. For more information about subscribers, see Subscribers, on page 405.

**Before you begin**

- Ensure the Microsoft Active Directory server does not reside behind a network address translator and does not have a Network Address Translation (NAT) address.
- Ensure the Microsoft Active Directory account intended for the join operation is valid and is not configured with the Change Password on Next Login.
- Ensure you have the privileges of a Super Admin or System Admin in ISE.
- Enable the Passive Identity and pxGrid services on the dedicated Policy server (PSN) you intend to use for any of the Passive Identity services — Choose Administration > System > Deployment, open the relevant node, and under General Settings, enable Enable Passive Identity Service and pxGrid.
- Ensure that ISE has an entry in the domain name server (DNS). Ensure you have properly configured reverse lookup for the client machine from ISE. For more information, see DNS Server, on page 328.

**Step 1** Choose Work Centers > PassiveID. From the Passive Identity Connector Overview screen, click Passive Identity Wizard.

The PassiveID Setup opens:
Step 2  Click **Next** to begin the wizard.

Step 3  From the Active Directory step, enter a unique name that distinguishes this configured Active Directory join point quickly and easily in Join Point Name, from Active Directory domain enter the domain name for the Active Directory Domain to which this node is connected, and enter your Active Directory administrator user name and password. For more information about these and other Active Directory settings, see *Active Directory Settings*, on page 365.

It is strongly recommended that you choose **Store credentials**, in which case your administrator's user name and password will be saved in order to be used for all Domain Controllers (DC) that are configured for monitoring.

Step 4  Click **Next** to define Active Directory groups and check any user groups to be included and monitored.
The Active Directory user groups automatically appear based on the Active Directory join point you configured in the previous step.

**Step 5**
Click **Next** again to move to the Domain Controllers step. From the Domain Controllers step, select the DCs to be monitored. If you choose Custom, then from the next screen select the specific DCs for monitoring. When finished, click **Next**.
Once you have selected specific DCs, you have finished creating your first Active Directory provider and the summary screen itemizes the DCs selected and their details.

**Step 6**
Click **Exit** to complete the wizard.

---

**What to do next**
When you finish configuring Active Directory as your initial provider, you can easily configure additional provider types as well. For more information, see Additional Passive Identity Service Providers, on page 368. Furthermore, you can now also configure a subscriber, designated to receive the user identity information that is collected by any of the providers you have defined. For more information, see Subscribers, on page 405.

**Manage the Active Directory Provider**
Once you have created and configured your Active Directory join points, continue to manage the Active Directory probe with these tasks:

- Test Users for Active Directory Authentication, on page 339
- View Active Directory Joins for a Node, on page 340
- Diagnose Active Directory Problems, on page 340
- Leave the Active Directory Domain, on page 331
- Delete Active Directory Configurations, on page 340
- Enable Active Directory Debug Logs, on page 341

**Active Directory Settings**
Active Directory (AD) is a highly secure and precise source from which to receive user information, including user name and IP address.
To create and manage Active Directory probes by creating and editing join points, choose Work Centers > PassiveID > Providers, from the left panel choose Active Directory.
For more information, see Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point, on page 329.

**Table 16: Active Directory Join Point Name Settings and Join Domain Screen**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Join Point Name</td>
<td>A unique name that distinguishes this configured join point quickly and easily.</td>
</tr>
<tr>
<td>Active Directory Domain</td>
<td>The domain name for the Active Directory Domain to which this node is connected.</td>
</tr>
</tbody>
</table>
**Field** | **Description**
---|---
Domain Administrator | This is the user principal name or the user account name for the Active Directory user with administrator privileges.
Password | This is the domain administrator's password as configured in Active Directory.
Specify Organizational Unit | Enter the administrator's organizational unit information.
Store Credentials | It is strongly recommended that you choose **Store credentials**, in which case your administrator's user name and password will be saved in order to be used for all Domain Controllers (DC) that are configured for monitoring.

For the Endpoint probe, you must choose **Store credentials**.

**Table 17: Active Directory Join/Leave Table**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISE Node</td>
<td>The URL for the specific node in the installation.</td>
</tr>
<tr>
<td>ISE Node Role</td>
<td>Indicates whether the node is the Primary or Secondary node in the installation.</td>
</tr>
<tr>
<td>Status</td>
<td>Indicates whether the node is actively joined to the Active Directory domain.</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>For nodes that are joined to Active Directory, this column indicates the specific Domain Controller to which the node is connected in the Active Directory Domain.</td>
</tr>
<tr>
<td>Site</td>
<td>When an Active Directory forest is joined with ISE, this field indicates the specific Active Directory site within the forest as it appears in the Active Directory Sites &amp; Services area.</td>
</tr>
</tbody>
</table>

Choose **Providers > Active Directory > PassiveID**.

**Table 18: Passive ID Domain Controllers (DC) List**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>The fully qualified domain name of the server on which the domain controller is located.</td>
</tr>
<tr>
<td>DC Host</td>
<td>The host on which the domain controller is located.</td>
</tr>
</tbody>
</table>
When an Active Directory forest is joined with ISE, this field indicates the specific Active Directory site within the forest as it appears in the Active Directory Sites & Services area.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site</td>
<td>When an Active Directory forest is joined with ISE, this field indicates the specific Active Directory site within the forest as it appears in the Active Directory Sites &amp; Services area.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the domain controller.</td>
</tr>
</tbody>
</table>
| Monitor Using| Monitor Active Directory domain controllers for user identity information by one of these methods:  
  - WMI—monitor Active Directory directly with the WMI infrastructure.  
  - Agent name—if you have defined agents to monitor Active Directory for user information, select the Agent protocol and choose the agent from the dropdown list that you would like to use. For more information about agents, see Active Directory Agents, on page 370. |

Choose Providers > Active Directory > PassiveID. Click the link for the AD join point to be edited, go to the PassiveID tab and click Edit to edit an existing Domain Controller from the list.

Table 19: Passive ID Domain Controllers (DC) Edit Screen

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host FQDN</td>
<td>Enter the fully qualified domain name of the server on which the domain controller is located.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a unique description for this domain controller in order to easily identify it.</td>
</tr>
<tr>
<td>User Name</td>
<td>The administrator's user name for accessing Active Directory.</td>
</tr>
<tr>
<td>Password</td>
<td>The administrator's password for accessing Active Directory.</td>
</tr>
</tbody>
</table>
| Protocol    | Monitor Active Directory domain controllers for user identity information by one of these methods:  
  - WMI—monitor Active Directory directly with the WMI infrastructure.  
  - Agent name—if you have defined agents to monitor Active Directory for user information, select the Agent protocol and choose the agent from the dropdown list that you would like to use. For more information about agents, see Active Directory Agents, on page 370. |
Table 20: Active Directory Groups

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory groups are defined and managed from Active Directory and the groups for the Active Directory that is joined to this node can be viewed from this tab. For more information about Active Directory, see <a href="https://msdn.microsoft.com/en-us/library/bb742437.aspx">https://msdn.microsoft.com/en-us/library/bb742437.aspx</a>.</td>
</tr>
</tbody>
</table>

Table 21: Active Directory Advanced Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>History interval</td>
<td>The time during which the Passive Identity service reads user login information that already occurred. This is required upon startup or restart of the Passive Identity service to catch up with events generated while it was unavailable. When the Endpoint probe is active, it maintains the frequency of this interval.</td>
</tr>
<tr>
<td>User session aging time</td>
<td>The amount of time the user can be logged in. The Passive Identity service identifies new user login events from the DC, however the DC does not report when the user logs off. The aging time enables Cisco ISE to determine the time interval for which the user is logged in.</td>
</tr>
<tr>
<td>NTLM Protocol settings</td>
<td>You can select either NTLMv1 or NTLMv2 as the communications protocol between Cisco ISE and the DC. NTLMv2 is the recommended default.</td>
</tr>
</tbody>
</table>

Additional Passive Identity Service Providers

In order to enable ISE to provide identity information (Passive Identity Service) to consumers that subscribe to the service (subscribers), you must first configure an ISE probe, which connects to the identity provider.

Providers that have been mapped and are actively delivering information to ISE can be viewed in the session directory, from the Live Sessions menu. For more information about Live Sessions, see RADIUS Live Sessions, on page 1156.

The table below provides details about all of the provider and probe types available from ISE, while the remainder of the chapter provides information regarding all types available except for Active Directory which is described in detail, in a dedicated chapter. For more information, see Active Directory as a Probe and a Provider, on page 362.

You can define these provider types:
## Table 22: Provider Types

<table>
<thead>
<tr>
<th>Provider Type (Probe)</th>
<th>Description</th>
<th>Source System (Provider)</th>
<th>Technology</th>
<th>User Identity Information Collected</th>
<th>Document Link</th>
</tr>
</thead>
</table>
| **Active Directory (AD)** | A highly secure and precise source, as well as the most common, from which to receive user information. As a probe, AD works with WMI technology to deliver authenticated user identities. In addition, AD itself, rather than the probe, functions as a source system (a provider) from which other probes retrieve user data as well. | Active Directory Domain Controller | WMI | • User name  
• IP address  
• Domain | Active Directory as a Probe and a Provider, on page 362 |
| **Agents** | A native 32-bit application installed on Active Directory domain controllers or on member servers. The Agent probe is a quick and efficient solution when using Active Directory for user identity information. | Agents installed on the domain controller or on a member server. | WMI | • User name  
• IP address  
• Domain | Active Directory Agents, on page 370 |
| **Endpoint** | Always runs in the background in addition to other configured probes, in order to verify whether the user is still connected. |  | WMI | Whether the user is still connected | Endpoint Probe, on page 403 |
| **SPAN** |  |  |  |  | SPAN, on page 379 |
### Active Directory Agents

From the Passive Identity service work center install the native 32-bit application, Domain Controller (DC) agents, anywhere on the Active Directory (AD) domain controller (DC) or on a member server (based on your configurations) to retrieve user identity information from AD and then send those identities to the subscribers you have configured. The Agent probe is a quick and efficient solution when using Active Directory for user identity information. Agents can be installed on a separate domain, or on the AD domain, and once installed, they provide status updates to ISE once every minute.

The agents can be either automatically installed and configured by ISE, or you can manually install them. Upon installation, the following occurs:

- The agent and its associated files are installed at the following path: **Program Files/Cisco/Cisco ISE PassiveID Agent**

- A config file called **PIAgent.exe.config** is installed indicating the logging level for the agent. You can manually change the logging level from within the config file.

- The CiscoISEPICAgent.log file is stored with all logging messages.

- The nodes.txt file contains the list of all nodes in the deployment with which the agent can communicate. The agent contacts the first node in the list. If that node cannot be contacted, the agent continues to attempt communication according to the order of the nodes in the list. For manual installations, you must
open the file and enter the node IP addresses. Once installed (manually or automatically), you can only change this file by manually updating it. Open the file and add, change or delete node IP addresses as necessary.

• The Cisco ISE PassiveID Agent service runs on the machine, which you can manage from the Windows Services dialog box.

• ISE supports up to 100 domain controllers, while each agent can monitor up to 10 domain controllers.

Note
In order to monitor 100 domain controllers, you must configure 10 agents.

Note
The Active Directory agents are only supported on Windows Server 2008 and higher.

If you cannot install agents, then use the Active Directory probe for passive identity services. For more information, see Active Directory as a Probe and a Provider, on page 362.

Automatically Install and Deploy Active Directory (AD) Agents

When configuring the Agent provider to monitor domain controllers for user identities, the agent must be installed on either a member server or on a domain controller. The agents can be either automatically installed by ISE, or you can manually install them. After installation, automatic or manual, you must then configure the installed agent to monitor specified domain controllers rather than the default WMI. This process describes how to enable automatic installation and configure the agent to monitor a domain controller.

Before you begin

Before you begin:

• Configure reverse lookup for the relevant DNS server/s from the server side. For more information about the DNS server configuration requirements for ISE, see DNS Server, on page 328.

• Ensure Microsoft .NET Framework is updated for the machine designated for the agents, to a minimum of version 4.0. For more information about the .NET framework, see https://www.microsoft.com/net/framework.

• Active Passive ID and pxGrid services. For more information, see Initial Setup and Configuration, on page 360.

• Create an AD join point and add at least one domain controller. For more information about creating join points, see Active Directory as a Probe and a Provider, on page 362.

Use AD user groups for the AD, Agents, SPAN and Syslog probes. For more information about AD groups, see Configure Active Directory User Groups, on page 333.

Step 1
Choose Work Centers > PassiveID > Providers and then choose Agents from the left panel to view all currently configured Domain Controller (DC) agents, to edit and delete existing agents, and to configure new agents.

Step 2
To add a new agent, click Add from the top of the table. To edit or change an existing client, checkmark the agent from the table and click Edit from the top of the table.
Manually Install and Deploy Active Directory (AD) Agents

When configuring the Agent provider to monitor domain controllers for user identities, the agent must be installed on either a member server or on a domain controller. The agents can be either automatically installed by ISE, or you can manually install them. After installation, automatic or manual, you must then configure the installed agent to monitor specified domain controllers rather than the default WMI. This process describes how to manually install and configure the agent to monitor a domain controller.

Before you begin

Before you begin:

- Configure reverse lookup for the relevant DNS server/s from the server side. For more information about the DNS server configuration requirements for ISE, see DNS Server, on page 328.
- Ensure Microsoft .NET Framework is updated for the machine designated for the agents, to a minimum of version 4.0. For more information about the .NET framework, see https://www.microsoft.com/net/framework.
- Active Passive ID and pxGrid services. For more information, see Initial Setup and Configuration, on page 360.
- Create an AD join point and add at least one domain controller. For more information about creating join points, see Active Directory as a Probe and a Provider, on page 362.

Use AD user groups for the AD, Agents, SPAN and Syslog probes. For more information about AD groups, see Configure Active Directory User Groups, on page 333.

Step 1

Choose Work Centers > PassiveID > Providers and then choose Agents from the left panel to view all currently configured Domain Controller (DC) agents, to edit and delete existing agents, and to configure new agents.

Step 2

Click Download Agent to download the picagent-installer.zip file for manual installation.
The file is downloaded to your standard Windows Download folder.

Step 3
Place the zip file on the designated host machine and run the installation.

Step 4
From the ISE GUI, again choose Work Centers > PassiveID > Providers and then choose Agents from the left panel.

Step 5
To configure a new agent, click Add from the top of the table. To edit or change an existing client, checkmark the agent from the table and click Edit from the top of the table.

Step 6
To configure the agent that you have already installed on the host machine, select Register Existing Agent.

Step 7
Complete all mandatory fields in order to configure the client correctly. For more information, see Active Directory (AD) Agent Settings, on page 373.

Step 8
Click Save.
The agent settings are saved. The agent now also appears in the Agents table and can be applied to monitor specified domain controllers, as described in the following steps.

Step 9
Choose Work Centers > PassiveID > Providers and then choose Active Directory from the left panel to view all currently configured join points.

Step 10
Click the link for the join point from which you would like to enable the agent you created.

Step 11
Choose the Passive ID tab in order to work with the domain controllers that you added as part of the prerequisites.

Step 12
Check mark the domain controller that you would like to monitor with the agent you created. and click Edit.

Step 13
From the dialog box that opens, ensure the mandatory fields are completed, from the Protocol dropdown select Agent, from the Agent field that appears, select the agent you created from the dropdown list, enter the user name and password credentials if you created any for the agent, and click Save.
The agent is enabled for the domain controller and the dialog box closes.

Uninstall the Agent

Agents, installed automatically or manually, can be easily (manually) uninstalled directly from Windows.

Step 1
From the Windows dialog, go to Programs and Features.

Step 2
Find and select the Cisco ISE PassiveID Agent in the list of installed programs.

Step 3
Click Uninstall.

Active Directory (AD) Agent Settings

Allow ISE to automatically install agents on a specified host in the network in order to retrieve user identity information from different Domain Controllers (DC) and deliver that information to Passive Identity service subscribers.

To create and manage agents, choose Providers > Agents. See Automatically Install and Deploy Active Directory (AD) Agents, on page 371.

View current agent statuses from the Agents table. Choose Providers > Agents.

Table 23: Agents Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The agent name as you configured it.</td>
</tr>
</tbody>
</table>
### API Providers

The API Providers feature in Cisco ISE enables you to push user identity information from your customized program or from the terminal server (TS)-Agent to the built-in ISE passive identity services REST API service. In this way, you can customize a programmable client from your network to send user identities that were collected from any network access control (NAC) system to the service. Furthermore, the Cisco ISE API provider enables you to interface with network applications such as the TS-Agent on a Citrix server, where all users have the same IP address but are assigned unique ports.

For example, an agent running on a Citrix server that provides identity mappings for users authenticated against an Active Directory (AD) server can send REST requests to ISE to add or delete a user session whenever a new user logs in or off. ISE then takes the user identity information, including the IP address and assigned
ports, delivered from the client and sends it to pre-configured subscribers, such as the Cisco Firepower Management Center (FMC).

The ISE REST API framework implements the REST service over the HTTPS protocol (no client certificate validation necessary) and the user identity information is delivered in JSON (JavaScript Object Notation) format. For more information about JSON, see http://www.json.org/.

The ISE REST API service parses user identities and in addition, maps that information to port ranges, in order to distinguish between the different users logged in simultaneously to one system. Everytime a port is allocated to a user, the API sends a message to ISE.

The REST API Provider Flow

Once you have configured a bridge to your customized client from ISE by declaring that client as a Provider for ISE and enabling that specific customized program (the client) to send RESTful requests, the ISE REST service works in the following way:

1. For client authentication, ISE requires an authentication token. A customized program on the client machine sends a request for an authentication token when initiating contact and then every time ISE notifies that the previous token has expired. The token is returned in response to the request, enabling ongoing communication between the client, and the ISE service.

2. Once a user has logged into the network, the client retrieves user identity information and posts that information to the ISE REST service using the API Add command.

3. ISE receives and maps the user identity information.

4. ISE sends the mapped user identity information to the subscriber.

5. Whenever necessary, the customized machine can send a request to remove user information by sending a Remove API call and including the user ID received as the response when the Add call was sent.

Work with REST API Providers in ISE

Follow these steps to activate the REST service in ISE:

1. Configure the client side. For more information, see the client user documentation.

2. Activate Passive ID and pxGrid services. For more information, see Initial Setup and Configuration, on page 360.

3. Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from ISE. For more information about the DNS server configuration requirements for, see DNS Server, on page 328.

4. See Configure a Bridge to the ISE REST Service for Passive Identity Services, on page 376.

Note

To configure the API Provider to work with a TS-Agent add the TS-Agent information when creating a bridge from ISE to that agent, and then consult with the TS-Agent documentation for information about sending API calls.

5. Generate an authentication token and send add and remove requests to the API service. #unique_575.
Configure a Bridge to the ISE REST Service for Passive Identity Services

In order to enable the ISE REST API service to receive information from a specific client, you must first define the specific client from ISE. You can define multiple REST API clients with different IP addresses.

Before you begin

Before you begin:

- Ensure you have activated Passive ID and pxGrid services. For more information, see Initial Setup and Configuration, on page 360.
- Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from ISE. For more information about the DNS server configuration requirements for ISE, see DNS Server, on page 328.

Step 1
Choose Work Centers > PassiveID > Providers and then choose API Providers from the left panel to view all currently configured clients, to edit and delete existing clients, and to configure new clients. The API Providers table is displayed, including status information for each existing client.

Step 2
To add a new client, click Add from the top of the table. To edit or change an existing client, checkmark the client from the table and click Edit from the top of the table.

Step 3
Complete all mandatory fields in order to configure the client correctly. For more information, see API Provider Settings, on page 377.

Step 4
Click Submit. The client configuration is saved and the screen displays the updated API Providers table. The client can now send posts to the ISE REST service.

What to do next

Set up your customized client to post authentication tokens and user identities to the ISE REST service. See Send API Calls to the Passive ID REST Service, on page 376.

Send API Calls to the Passive ID REST Service

Before you begin

Configure a Bridge to the ISE REST Service for Passive Identity Services, on page 376.

Step 1
Enter the Cisco ISE URL in the address bar of your browser (for example, https://<ise hostname or ip address>/admin/)

Step 2
Enter the username and password that you specified and configured from the API Providers screen in the ISE GUI. For more information, see Configure a Bridge to the ISE REST Service for Passive Identity Services, on page 376.

Step 3
Press Enter.

Step 4
Enter the API call in the URL Address field of the target node as follows:

Step 5
Click Send to issue the API call.
What to do next

See API Calls, on page 377 for more information and details about the different API calls, their schemas and their results.

API Provider Settings

Choose Providers > API Providers to configure a new REST API client for s.

Note

The full API definition and object schemas can be retrieved with a request call as follows:

- For the full API specifications (wadl)—https://YOUR_ISE:9094/application.wadl
- For the API model and object schemas—https://YOUR_ISE:9094/application.wadl/xsd0.xsd

Table 25: API Providers Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name for this client that distinguishes it quickly and easily from other clients.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a clear description of this client.</td>
</tr>
<tr>
<td>Status</td>
<td>Select Enabled to enable the client to interact with the REST services immediately upon completing configuration.</td>
</tr>
<tr>
<td>Host/IP</td>
<td>Enter the IP address for the client host machine. Ensure you have properly configured the DNS server, including configuring reverse lookup for the client machine from ISE.</td>
</tr>
<tr>
<td>User name</td>
<td>Create a unique user name to be used when posting to the REST service.</td>
</tr>
<tr>
<td>Password</td>
<td>Create a unique password to be used when posting to the REST service.</td>
</tr>
</tbody>
</table>

API Calls

Use these API calls to manage user identity events for Passive Identity services with Cisco ISE.

Purpose: Generate Authentication Token

- Request

  POST

  https://<PIC IP address>:9094/api/fmi_platform/v1/identityauth/generatetoken
The request should contain the BasicAuth authorization header—provide the API provider's credentials as previously created from the ISE-PIC GUI. For more information see API Provider Settings, on page 377.

- **Response Header**
  
The header includes the X-auth-access-token. This is the token to be used when posting additional REST requests.

- **Response Body**
  
  HTTP 204 No Content

**Purpose: Add User**

- **Request**
  
  POST
  
  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity
  
  Add X-auth-access-token in the header of the POST request. (For example, Header: X-auth-access-token, Value: f3f25d81-3ac5-43ee-bbfb-20955643f6a7)

- **Response Header**
  
  201 Created

- **Response Body**
  
  
```
{
  "user": "<username>",
  "srcPatRange": {
    "userPatStart": "<user PAT start value>",
    "userPatEnd": "<user PAT end value>",
    "patRangeStart": "<PAT range start value>
  },
  "srcIpAddress": "<src IP address>",
  "agentInfo": "<Agent name>",
  "timestamp": "<ISO_8601 format i.e. YYYY-MM-DDTHH:MM:SSZ>",
  "domain": "<domain>
}
```

- **Notes**
  
  - srcPatRange can be removed in above json to create a single IP user binding.

  - Response body contains the "ID" which is the unique identifier for the user session binding created. Use this ID when sending a DELETE request to indicate which user should be removed.

  - This response also contains the self link which is the URL for this newly created user session binding.
Purpose: Remove User

• Request
  DELETE
  https://<PIC IP address>:9094/api/identity/v1/identity/useridentity/<id>
  In <id> enter the ID as was received from the Add response.
  Add the X-auth-access-token in the header of the DELETE request. (For example, Header:
  X-auth-access-token, Value: f3f25d81-3ac5-43ee-bbfb-20955643f6a7)

• Response Header
  200 OK

• Response Body
  Response body contains the details about the user session binding which got deleted.

SPAN

SPAN is a Passive Identity service that allows you to quickly and easily enable ISE to listen to the network and retrieve user information without having to configure Active Directory to work directly with ISE. SPAN sniffs network traffic, specifically examining Kerberos messages, extracts user identity information also stored by Active Directory and sends that information to ISE. ISE then parses the information, ultimately delivering user name, IP address and domain name to the subscribers that you have also already configured from ISE.

In order for SPAN to listen to the network and extract Active Directory user information, ISE and Active Directory must both be connected to the same switch on the network. In this way, SPAN can copy and mirror all user identity data from Active Directory.

With SPAN, user information is retrieved in the following way:

1. The user endpoint, on the network, logs in.
2. Login and user data are stored in Kerberos messages.
3. Once the user logs in and the user data passes through the switch, SPAN mirrors the network data.
4. ISE listens to the network for user information and retrieves the mirrored data from the switch.
5. ISE parses the user information and updates passive ID mappings.
6. ISE delivers the parsed user information to the subscribers.

Working with SPAN

Before you begin

In order to enable ISE to receive SPAN traffic from a network switch, you must first define which nodes and node interfaces are to listen to the switch. You can configure SPAN in order to listen to the different installed ISE nodes. For each node, only one interface can be configured to listen to the network and the interface used to listen must be dedicated to SPAN only.
Before you begin, ensure you have activated Passive ID and pxGrid services. Only nodes for which Passive ID has been turned on will appear in the list of available interfaces for configuring SPAN. For more information, see Initial Setup and Configuration, on page 360.

In addition, you must:

- Ensure Active Directory is configured on your network.
- Run a CLI on the switch in the network that is also connected to Active Directory in order to ensure the switch can communicate with ISE.
- Configure the switch to mirror the network from AD.
- Configure a dedicated ISE network interface card (NIC) for SPAN. This NIC is used only for SPAN traffic.
- Ensure the NIC that you have dedicated to SPAN is activated via the command line interface.
- Create a VACL that sends only Kerberos traffic into the SPAN port.

**Step 1**
Choose Work Centers > PassiveID > Providers and then choose SPAN from the left panel to configure SPAN.

**Step 2**
Note
It is recommended that the GigabitEthernet0 network interface card (NIC) remain available and that you select any other available NIC for configuring SPAN. GigabitEthernet0 is used for system management purposes.

Enter a meaningful description (optional), select status **Enabled**, and choose the nodes and the relevant NICs that will be used to listen to the network switch. For more information, see SPAN Settings, on page 380.

**Step 3**
Click **Save**.
The SPAN configuration is saved and ISE-PIC ISE is now actively listening to network traffic.

**SPAN Settings**

From each node that you have deployed, quickly and easily configure ISE to receive user identities by installing SPAN on a client network.

**Table 26: SPAN Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a unique description to remind you of which nodes and interfaces are currently enabled.</td>
</tr>
<tr>
<td>Status</td>
<td>Select <strong>Enabled</strong> to enable the client immediately upon completing configuration.</td>
</tr>
</tbody>
</table>
Select one or more of the nodes installed for ISE, and then for each selected node, choose the node interface that is to listen to the network for information.

**Note**  
It is recommended that the GigabitEthernet0 NIC remain available and that you select any other available NIC for configuring SPAN. GigabitEthernet0 is used for system management purposes.

### Syslog Providers

With the Syslog feature, the Passive Identity service parses syslog messages from any client (identity data provider) that delivers syslog messages, including regular syslog messages (from providers such as InfoBlox, Blue Coat, BlueCat, and Lucent) as well as DHCP syslog messages, and sends back user identity information, including MAC addresses. This mapped user identity data is then delivered to subscribers.

The Passive Identity service utilizes syslog messages received from a variety of providers once the administrator activates Passive ID and pxGrid services and configures the syslog client from the GUI. When configuring the provider, the administrator indicates the connection method (TCP or UDP) and the syslog template to be used for parsing.

**Note**  
When TCP is the configured connection type, if there is a problem with the message header and the host name cannot be parsed, then ISE attempts to match the IP address received in the packet to the IP address of any of the providers in the list of providers that have already been configured for Syslog messages in ISE. To view this list, choose **Work Centers > PassiveID > Providers > Syslog Providers**. It is recommended that you check the message headers and customize if necessary in order to guarantee parsing succeeds. For more information about customizing headers, see Customize Syslog Headers, on page 388.

Once configured, the syslog probe sends syslog messages that are received to the ISE parser, which maps the user identity information, and publishes that information to ISE. ISE then delivers the parsed and mapped user identity information to the Passive Identity service subscribers.

**Note**  
DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that ISE can first check users registered in the local session directory (displayed from Live Sessions) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, in order to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message is not parsed and user identity is not delivered.

In order to parse syslog messages for user identity from ISE:

- Configure syslog clients from which to receive user identity data—Configure Syslog Clients, on page 382
- Customize a single message header—Customize Syslog Headers, on page 388
Configure Syslog Clients

In order to enable ISE to listen to syslog messages from a specific client, you must first define the specific client from ISE. You can define multiple providers with different IP addresses.

**Before you begin**

Before you begin, ensure you have activated Passive ID and pxGrid services. For more information, see Initial Setup and Configuration, on page 360.

| Step 1 | Choose **Work Centers > PassiveID > Providers** and then choose **Syslog Providers** from the left panel to view all currently configured clients, to edit and delete existing clients, and to configure new clients. The Syslog Providers table is displayed, including status information for each existing client. |
| Step 2 | To configure a new syslog client, click **Add** from the top of the table. To edit or change a previously configured client, checkmark the client from the table and click **Edit** from the top of the table. |
| Step 3 | Complete all mandatory fields (see Syslog Settings, on page 382 for more details) and create a message template if necessary (see Customize the Syslog Message Body, on page 387 for more details) in order to configure the client correctly. |
| Step 4 | Click **Submit**. The client configuration is saved and the screen displays the updated Syslog Providers table. |

**Syslog Settings**

Configure ISE to receive user identities, including MAC addresses, by way of syslog messages from a specific client. You can define multiple providers with different IP addresses.

Choose **Work Centers > PassiveID > Providers**, from the left panel choose **Syslog Providers** and from the table click **Add** to create a new syslog client.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name that distinguishes this configured client quickly and easily.</td>
</tr>
<tr>
<td>Description</td>
<td>A meaningful description of this Syslog provider.</td>
</tr>
<tr>
<td>Status</td>
<td>Select <strong>Enabled</strong> to enable the client immediately upon completing configuration.</td>
</tr>
<tr>
<td>Host</td>
<td>Enter the FQDN of the host machine.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Connection Type</td>
<td>Enter UDP or TCP to indicate the channel by which ISE listens for syslog messages.</td>
</tr>
</tbody>
</table>

**Note** When TCP is the configured connection type, if there is a problem with the message header and the host name cannot be parsed, then ISE-PIC ISE attempts to match the IP address received in the packet to the IP address of any of the providers in the list of providers that have already been configured for Syslog messages in ISE-PIC ISE.

To view this list, choose **Work Centers > PassiveID > Providers > Syslog Providers**. It is recommended that you check the message headers and customize if necessary in order to guarantee parsing succeeds. For more information about customizing headers, see **Customize Syslog Headers, on page 388**.
### Syslog Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td></td>
</tr>
</tbody>
</table>
A template indicates precise body message structure so that the parser can identify the pieces of information within the syslog message that should be parsed, mapped and delivered.

For example, a template can indicate the exact position of the user name so that the parser can find the user name in every message received.

From this field, indicate the template (for the body of the syslog message) to be used in order to recognize and correctly parse the syslog message.

Choose either from the pre-defined dropdown list, or click **New** to create your own customized template. For more information about creating new templates, see [Customize the Syslog Message Body, on page 387](#). Most of the pre-defined templates use regular expressions, and customized templates should also use regular expressions.

**Note** Only customized templates can be edited or removed, while pre-defined system templates in the dropdown cannot be altered.

ISE currently offers these pre-defined DHCP provider templates:

- InfoBlox
- BlueCat
- Lucent_QIP
- DHCPD
- MSAD DHCP

**Note** DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that ISE-PIC ISE can first check users registered in the local session directory (displayed from Live Sessions) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, in order to correctly parse and deliver user identity information.

If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
|       | A template indicates precise body message structure so that the parser can identify the pieces of information within the syslog message that should be parsed, mapped and delivered. For example, a template can indicate the exact position of the user name so that the parser can find the user name in every message received. From this field, indicate the template (for the body of the syslog message) to be used in order to recognize and correctly parse the syslog message. Choose either from the pre-defined dropdown list, or click New to create your own customized template. For more information about creating new templates, see [Customize the Syslog Message Body, on page 387](#). Most of the pre-defined templates use regular expressions, and customized templates should also use regular expressions. **Note** Only customized templates can be edited or removed, while pre-defined system templates in the dropdown cannot be altered. ISE currently offers these pre-defined DHCP provider templates:  
- InfoBlox  
- BlueCat  
- Lucent_QIP  
- DHCPD  
- MSAD DHCP  
**Note** DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that ISE-PIC ISE can first check users registered in the local session directory (displayed from Live Sessions) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, in order to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message |
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>is not parsed and user identity is not delivered.</td>
</tr>
<tr>
<td></td>
<td>ISE offers these pre-defined regular syslog provider templates:</td>
</tr>
<tr>
<td></td>
<td>• ISE</td>
</tr>
<tr>
<td></td>
<td>• ACS</td>
</tr>
<tr>
<td></td>
<td>• F5_VPN</td>
</tr>
<tr>
<td></td>
<td>• ASA_VPN</td>
</tr>
<tr>
<td></td>
<td>• Blue Coat</td>
</tr>
<tr>
<td></td>
<td>• Aerohive</td>
</tr>
<tr>
<td></td>
<td>• Safe connect_NAC</td>
</tr>
<tr>
<td></td>
<td>• Nortel_VPN</td>
</tr>
</tbody>
</table>

For information about templates, see **Work with Syslog Pre-Defined Message Templates, on page 391**.

<table>
<thead>
<tr>
<th>Default Domain</th>
<th>If the domain is not identified in the syslog message for the specific user, this default domain is automatically assigned to the user in order to ensure that all users are assigned a domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>With the default domain or with the domain that was parsed from the message, the user name is appended to username@domain, thereby including that domain, in order to get more information about the user and user groups.</td>
</tr>
</tbody>
</table>

**Customize Syslog Message Structures (Templates)**

A template indicates precise message structure so that the parser can identify the pieces of information within the syslog message that should be parsed, mapped and delivered. For example, a template can indicate the exact position of the user name so that the parser can find the user name in every message received. Templates determine the supported structures for both new and remove mapping messages.

Cisco ISE enables you to customize a single message header and multiple body structures, to be used by the Passive ID parser.

The templates should include regular expressions to define the structure for user name, IP address, MAC address and domain in order to enable the Passive ID parser to correctly identify whether the message is to add or remove user identity mapping and to correctly parse the user details.

When customizing your message templates, you can choose to base your customization on the message templates pre-defined in ISE-PIC ISE by consulting with the regular expressions and message structures used within those pre-defined options. For more information about the pre-defined template regular expressions, message structures, examples and more, see **Work with Syslog Pre-Defined Message Templates, on page 391**.
You can customize:

- A single message header—Customize Syslog Headers, on page 388
- Multiple message bodies—Customize the Syslog Message Body, on page 387.

---

**Note**

DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that ISE-PIC ISE can first check users registered in the local session directory (displayed from Live Sessions) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, in order to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message is not parsed and user identity is not delivered.

The delay necessary to properly match, parse and map details from DHCP messages cannot be applied to customized templates, and therefore it is not recommended that DHCP message templates be customized. Instead, use any of the pre-defined DHCP templates.

---

**Customize the Syslog Message Body**

Cisco ISE enables you to customize your own syslog message templates (by customizing the message body) to be parsed by the Passive ID parser. The templates should include regular expressions to define the structure for user name, IP address, MAC address and domain.

---

**Note**

DHCP syslog messages do not contain user names. Therefore, these messages are delivered from the parser with a delay so that ISE-PIC ISE can first check users registered in the local session directory (displayed from Live Sessions) and attempt to match those users by their IP addresses to the IP addresses listed in the DHCP syslog messages received, in order to correctly parse and deliver user identity information. If the data received from a DHCP syslog message cannot be matched to any of the currently logged in users, then the message is not parsed and user identity is not delivered.

The delay necessary to properly match, parse and map details from DHCP messages cannot be applied to customized templates, and therefore it is not recommended that DHCP message templates be customized. Instead, use any of the pre-defined DHCP templates.

Create and edit syslog message body templates from within the syslog client configuration screen.

---

**Note**

You can only edit your own customized templates. Pre-defined templates offered by the system cannot be changed.

---

**Step 1**

Choose Work Centers > PassiveID > Providers and then choose Syslog Providers from the left panel to view all currently configured clients, to edit and delete existing clients, and to configure new clients. The Syslog Providers table is displayed, including status information for each existing client.

**Step 2**

Click Add to add a new syslog client or Edit to update an already configured client. If you only want to add or edit a template, it doesn't matter which of these options you select. For more information about configuring and updating syslog clients, see Configure Syslog Clients, on page 382.
Step 3  From the Syslog Providers screen, next to the Template field, click New to create a new message template. To edit an existing template, select the template from the dropdown list and click Edit. The Syslog Template screen opens.

Step 4  Complete all mandatory fields.

For information about how to enter the values correctly, see Syslog Customized Template Settings and Examples, on page 389.

Step 5  Click Test to ensure the message is correctly parsed based on the strings you have entered.

Step 6  Click Save.

The customized template is saved and now appears in the dropdown list from the Template field when configuring new and updating existing syslog clients.

Customize Syslog Headers

Syslog headers, amongst other details, also contain the hostname from which the message originated. If your syslog messages are not recognized by the ISE message parser, you may need to customize the message header by configuring the delimiter that proceeds the host name, thereby enabling ISE to recognize the host name and parse the message correctly. For more details about the fields in this screen, see Syslog Customized Template Settings and Examples, on page 389. The customized header configuration is saved and added to the header types that are used by the parser whenever messages are received.

Note  You can only customize a single header. Once you customize a header, when you click Custom Header, create a template to be stored and click Submit, the newest configuration is saved and overrides the previous customization.

---

Step 1  Choose Work Centers > PassiveID > Providers and then choose Syslog Providers from the left panel to view all currently configured clients, to edit and delete existing clients, and to configure new clients. The Syslog Providers table is displayed, including status information for each existing client.

Step 2  Click Custom Header to open the Syslog Custom Header screen.

Step 3  From the Paste sample syslog enter an example of the header format in your syslog messages. For example, copy and paste this header from one of your messages: <181>Oct 10 15:14:08 Cisco.com.

Step 4  From the Separator field, indicate whether words are separated by spaces or tabs.

Step 5  From the Position of hostname in header field, indicate which place in the header is the hostname. For example, in the header offered above, the hostname is the fourth word in the header. Enter 4 to indicate this.

The Hostname field displays the host name based on the details indicated in the first three fields. For example, if the header example in Paste sample syslog is as follows:

<181>Oct 10 15:14:08 Cisco.com

The separator is indicated as Space and the Position of hostname in header is entered as 4.

The Hostname will automatically appear as Cisco.com, which is the fourth word in the header phrase pasted in the Paste sample syslog field.

If the host name is incorrectly displayed, check the data you have entered in the Separator and Position of hostname in header fields.
This example is as in the following screen capture:

*Figure 33: Customize Syslog Headers*

**Syslog Custom Header**

If some or all of the syslog messages are not being accepted, it may be because they have an uncommon header format. Define a custom header here.

- **Paste sample syslog:** `<181>Oct 10 15:14:08 Hostname Message`
- **Separator:** `Space`
- **Position of hostname in header:** `4`
- **Hostname:** Hostname

Click **Submit**.
The customized header configuration is saved and added to the header types that are used by the parser whenever messages are received.

---

**Step 6**  
**Note**  
You can only customize a single header. Once you customize a header, when you click **Custom Header**, create a template to be stored and click **Submit**, the newest configuration is saved and overrides the previous customization.

**Step 6**  
**Note**  
You can only customize a single header. Once you customize a header, when you click **Custom Header**, create a template to be stored and click **Submit**, the newest configuration is saved and overrides the previous customization.

---

**Syslog Customized Template Settings and Examples**

Cisco ISE enables you to customize your own syslog message templates to be parsed by the Passive ID parser. Customized templates determine the supported structures for both new and remove mapping messages. The templates should include regular expressions to define the structure for user name, IP address, MAC address and domain in order to enable the Passive ID parser to correctly identify whether the message is to add or remove user identity mapping and to correctly parse the user details.

---

**Note**

Most of the pre-defined templates use regular expressions. Customized templates should also use regular expressions.

---

**Syslog Header Parts**

You can customize a single header that is recognized by the Syslog probe by configuring the delimiter that proceeds the host name.

Choose **Work Centers > PassiveID > Providers**, from the left panel choose **Syslog Providers** and from the table click **Custom Header** to create a customized syslog message header.
The following table describes the different parts and fields that can be included in your customized syslog header. For more information about regular expressions, see Table 30: Regular Expressions for Customized Templates, on page 391.

**Table 28: Syslog Custom Header**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paste sample syslog</td>
<td>Enter an example of the header format in your syslog messages. For example, copy and paste this header: (&lt;181&gt;Oct 10 15:14:08 Hostname Message)</td>
</tr>
<tr>
<td>Separator</td>
<td>Indicate whether words are separated by spaces or tabs.</td>
</tr>
<tr>
<td>Position of hostname in header</td>
<td>Indicate which place in the header is the host name. For example, in the header offered above, the host name is the fourth word in the header. Enter 4 to indicate this.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Displays the hostname based on the details indicated in the first three fields. For example, if the header example in Paste sample syslog is as follows: (&lt;181&gt;Oct 10 15:14:08 Hostname Message) The separator is indicated as Space and the Position of hostname in header is entered as 4. The Hostname will automatically appear as Hostname. If the host name is incorrectly displayed, check the data you have entered in the Separator and Position of hostname in header fields.</td>
</tr>
</tbody>
</table>

**Syslog Template Parts and Descriptions for the Message Body**

The following table describes the different parts and fields that can be included in your customized syslog message templates. For more information about regular expressions, see Table 30: Regular Expressions for Customized Templates, on page 391.

**Table 29: Syslog Template**

<table>
<thead>
<tr>
<th>Part</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name</td>
<td>A unique name by which to recognize the purpose of this template.</td>
</tr>
</tbody>
</table>
### Regular Expression Examples

In order to parse messages use regular expressions. This sections offers regular expression examples in order to parse IP address, user name and add mapping messages.

For example, use regular expressions to parse the following messages:

- `<174>192.168.0.1 %ASA-4-722051: Group <DfltGrpPolicy> User <user1> IP <192.168.0.10> IPv4 Address <192.168.0.6> IPv6 address <::> assigned to session
- `<174>192.168.0.1 %ASA-6-713228: Group = xyz, Username = user1, IP = 192.168.0.12, Assigned private IP address 192.168.0.8 to remote user

The regular expressions are as defined in the following table.

**Table 30: Regular Expressions for Customized Templates**

<table>
<thead>
<tr>
<th>Part</th>
<th>Regular Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address</td>
<td>Address &lt;([^\s]+)&gt;</td>
</tr>
<tr>
<td>User name</td>
<td>User &lt;([^\s]+)&gt;</td>
</tr>
<tr>
<td>Add mapping message</td>
<td>(%ASA-4-722051</td>
</tr>
</tbody>
</table>

### Work with Syslog Pre-Defined Message Templates

Syslog messages have a standard structure which include a header and the message body.

The pre-defined templates offered by Cisco ISE are described in this section, including content details for the headers that are supported, as well as the supported body structure, based on the origin of the messages.
In addition, you can create your own templates with customized body content for sources that are not pre-defined in the system. The supported structure for customized templates is also described in this section. You can configure a single customized header to be used in addition to the headers pre-defined in the system, when parsing messages, and you can configure multiple customized templates for the message body. For more information about customizing the header, see Customize Syslog Headers, on page 388. For more information about customizing the body, see Customize the Syslog Message Body, on page 387.

Note
Most of the pre-defined templates use regular expressions, and customized templates should also use regular expressions.

Message Headers
There are two header types recognized by the parser, for all message types (new and remove), for all client machines. These headers are as follows:

• <171>Host message
• <171>Oct 10 15:14:08 Host message

Once received, the header is parsed for host name, which can be IP address, hostname, or full FQDN. Headers can also be customized. To customize your headers, see Customize Syslog Headers, on page 388.

Syslog ASA VPN Pre-Defined Template
The supported syslog message format and types for ASA VPN are as described below.

Headers
Headers supported by the parser are identical for all clients, as described in Work with Syslog Pre-Defined Message Templates, on page 391.

New Mapping Body Messages
There are different ASA VPN body messages that are recognized by the parser as described in the following table.
### Body Message

| %ASA-6-109005 Authentication succeeded for user UserA from 10.0.0.11/100 to 10.10.11/20 on interface eth1/1 |
| %ASA-6-602303 IPSEC: An direction tunnel_type SA (SPI=spi) between local_IP and 10.0.0.11 (UserA) has been created. |
| %ASA-6-721016 (device) WebVPN session for client user UserA, IP 10.0.0.11 has been created. |
| %ASA-6-603104 PPTP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number, client_dynamic_ip is 10.0.0.11, fgg123 # UserA is UserA, MPPE_key_strength is string |
| %ASA-6-603106 L2TP Tunnel created, tunnel_id is number, remote_peer_ip is remote_address, ppp_virtual_interface_id is number, client_dynamic_ip is 10.0.0.11, UserA is user |
| %ASA-6-113039 Group group User UserA IP 10.0.0.11 AnyConnect parent session started. |
| %ASA-6-802001 User UserA IP 10.100.1.1 OS os_name UDID number MDM action session started. |

### Parsing Example

| [UserA,10.0.0.11] |
| [UserA,172.16.0.12] |

---

### Remove Mapping Body Messages

The Remove Mapping messages supported for ASA VPN by the parser are as described in this section.

Once received, the body is parsed for user details as follows:

| [UserA,10.1.1.1] |

---

| %ASA-4-113019 Group = group, UserA = UserA, IP = 10.1.1.1, Session disconnected. Session Type: type, Duration: duration, Bytes xmt: count, Bytes rcv: count, Reason: reason |

| [UserA,172.16.0.11] |

**Note** The parsed IP address from this message type is the private IP address, as indicated in the message.

| [UserA,172.16.0.12] |

**Note** The parsed IP address from this message type is the IPv4 address.
### Body Message

- **%ASA-4-717052** Group group name User UserA IP 10.1.1.1 Session disconnected due to periodic certificate authentication failure. Subject Name id subject name Issuer Name id issuer name\ Serial Number id serial number

- **%ASA-6-602304** IPSEC: An direction tunnel_type SA (SPI=sdpi) between local_IP and 10.1.1.1 (UserA) has been deleted.

- **%ASA-6-721018** WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

- **%ASA-4-722049** Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled or invalid image on the ASA

- **%ASA-4-722050** Group group User UserA IP 10.1.1.1 Session terminated: SVC not enabled for the user.

- **%ASA-6-802002** User UserA IP 10.1.1.1 OS os_name UDID number MDM action session terminated.

- **%ASA-3-716057** Group group User UserA IP 10.1.1.1 Session terminated, no type license available.

- **%ASA-3-722046** Group group User UserA IP 10.1.1.1 Session terminated: unable to establish tunnel.

- **%ASA-4-113035** Group group User UserA IP 10.1.1.1 Session terminated: AnyConnect not enabled or invalid AnyConnect image on the ASA.

- **%ASA-4-716052** Group group-name User UserA IP 10.1.1.1 Pending session terminated.

- **%ASA-6-721018** WebVPN session for client user UserA, IP 10.1.1.1 has been deleted.

---

### Syslog Bluecat Pre-Defined Template

The supported syslog message format and types for Bluecat are as described below.

#### Headers

Headers supported by the parser are identical for all clients, as described in [Work with Syslog Pre-Defined Message Templates](#), on page 391.

#### New Mapping Body Messages

The messages supported for New Mapping for Bluecat syslog are as described in this section.

Once received, the body is parsed for user details as follows:

```plaintext
```

#### Body


#### Remove Mapping Messages

There are no remove mapping messages known for Bluecat.
Syslog F5 VPN Pre-Defined Template

The supported syslog message format and types for F5 VPN are as described below.

**Headers**

Headers supported by the parser are identical for all clients, as described in [Work with Syslog Pre-Defined Message Templates, on page 391](#).

**New Mapping Body Messages**

There are different F5 VPN body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

```
[user=UserA, ip=172.16.0.12]
```

**Body**

<table>
<thead>
<tr>
<th>Body Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 10 09:33:58 Oct 2 08:28:32 abc.xyz.org security[nnnnn]: [UserA@vendor-abc] User A logged on from 172.16.0.21 to 172.16.0.12 Sid = xyz</td>
</tr>
</tbody>
</table>

**Remove Mapping Messages**

Currently there are no remove messages for F5 VPN that are supported.

Syslog Infoblox Pre-Defined Template

The supported syslog message format and types for Infoblox are as described below.

**Headers**

Headers supported by the parser are identical for all clients, as described in [Work with Syslog Pre-Defined Message Templates, on page 391](#).

**New Mapping Body Messages**

There are different ASA VPN body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

```
[macAddress= nn:xx:xx:xx:nn:nn, ip=10.0.10.100]
```

**Body Message**

<table>
<thead>
<tr>
<th>Body Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nov 15 11:37:26 user1-lnx dhcpd[3179]: DHCPACK on 10.0.0.14 to nn:xx:xx:nn:nn (android-df67ddeb1271593) via eth2 relay 10.0.0.24 lease-duration 3600</td>
</tr>
<tr>
<td>Nov 15 11:38:11 user1-lnx dhcpd[3179]: DHCPACK on 172.16.0.18 to nn:xx:xx:nn:nn (DESKTOP-HUDGAAG) via eth2 relay 172.16.0.13 lease-duration 691200 (RENEW)</td>
</tr>
</tbody>
</table>
Remove Mapping Messages

The following messages are supported for Remove Mapping.

There are several body messages recognized by the parser for remove mapping messages, as described in the table below.

Once received, the body is parsed for user details as follows:

- If MAC address is included:
  \[00:0c:29:a2:18:34,10.0.10.100]\n
- If MAC address is not included:
  \[10.0.10.100]\n
Syslog Linux DHCPd3 Pre-Defined Template

The supported syslog message format and types for Linux DHCPd3 are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Pre-Defined Message Templates, on page 391.

New Mapping Messages

There are different Linux DHCPd3 body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

\[\text{macAddress}=24:ab:81:ca:f2:72,\text{ip}=172.16.0.21\]

Remove Mapping Body Messages

The Remove Mapping messages supported for Linux DHCPd3 by the parser are as described in this section.

Once received, the body is parsed for user details as follows:
Syslog MS DHCP Pre-Defined Template

The supported syslog message format and types for MS DHCP are as described below.

**Headers**

Headers supported by the parser are identical for all clients, as described in Work with Syslog Pre-Defined Message Templates, on page 391.

**New Mapping Body Messages**

There are different MS DHCP body messages that are recognized by the parser as described in the following table.

Once received, the parser divides data by searching for the comma (,) and then messages of these formats are parsed as in the following example:

```
[00:0c:29:a2:18:34 ,10.0.10.100]

Body Message
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1
```

**Remove Mapping Body Messages**

The Remove Mapping messages supported for MS DHCP by the parser are as described in this section.

Once received, the parser divides data by searching for the comma (,) and then messages of these formats are parsed as in the following example:

```
[00:0c:29:a2:18:34 ,10.0.10.100]

Body Message
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPEXPIRE 10.0.10.100 has expired
Nov 11 23:37:32 dhcpsrv dhcpd: DHCPRELEASE of 10.0.10.100 from 00:0c:29:a2:18:34 (win10) via eth1
```

Syslog SafeConnect NAC Pre-Defined Template

The supported syslog message format and types for SafeConnect NAC are as described below.

**Headers**

Headers supported by the parser are identical for all clients, as described in Work with Syslog Pre-Defined Message Templates, on page 391.
New Mapping Body Messages

There are different SafeConnect NAC body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

[user=galindk1i,p=xxxx.xx.xxx.xxd,domain=Resnet-Macs]

<table>
<thead>
<tr>
<th>Body Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 10 09:33:58 nac Safe*Connect: authenticationResult</td>
</tr>
</tbody>
</table>

Remove Mapping Messages

Currently there are no remove messages for Safe Connect that are supported.

Syslog Aerohive Pre-Defined Templates

The supported syslog message format and types for Aerohive are as described below.

Headers

Headers supported by the parser are identical for all clients, as described in Work with Syslog Pre-Defined Message Templates, on page 391.

New Mapping Body Messages

There are different Aerohive body messages that are recognized by the parser as described in the following table.

Details parsed from the body include username and IP address. The regular expression used for parsing is as in the following examples:

• New mapping-auth:
• IP-ip (\{A-F0-9a-f.:\}+)
• User name-UserA (\{a-zA-Z0-9_/\}+)

Once received, the body is parsed for user details as follows:

[UserA,10.5.50.52]

<table>
<thead>
<tr>
<th>Body Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013-04-01 14:06:05 info ah auth: Station 1cab:a7e6:cf7f ip 10.5.50.52 UserA UserA</td>
</tr>
</tbody>
</table>

Remove Mapping Messages

Currently the system does not support remove mapping messages from Aerohive.

Syslog Blue Coat Pre-Defined Templates—Main Proxy, Proxy SG, Squid Web Proxy

The system supports the following message types for Blue Coat:

• BlueCoat Main Proxy
• BlueCoat Proxy SG
• BlueCoat Squid Web Proxy

The supported syslog message format and types for Bluecoat messages are as described below.

**Headers**

Headers supported by the parser are identical for all clients, as described in Work with Syslog Pre-Defined Message Templates, on page 391.

**New Mapping Body Messages**

There are different Blue Coat body messages that are recognized by the parser as described in the following table.

Once received, the body is parsed for user details as follows:

[UserA.192.168.10.24]

**Body Message (this example is taken from a BlueCoat Proxy SG message)**

| 2016-09-21 23:05:33 58 10.0.0.1 UserA - - PROXIED "none" http://www.example.com/ 200 TCP_MISS GET application/json;charset=UTF-8 httpsite.api.example.com80/apis/v2/scoreboard/header?rand=1474499133503 - "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2486.0 Safari/537.36 Edge/13.10586" 192.168.10.24 7186 708 - "unavailable |

The following table describes the different regular expression structures used per client for new mapping messages.

<table>
<thead>
<tr>
<th>Client</th>
<th>Regular expressions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BlueCoat Main Proxy</td>
<td>New mapping (TCP_HIT</td>
</tr>
<tr>
<td>BlueCoat Proxy SG</td>
<td>New mapping (\sPROXIED){1} IP ([0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}) User name ([a-zA-Z0-9_]+</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Client</th>
<th>Regular expressions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BlueCoat Squid Web Proxy</td>
<td>New mapping</td>
</tr>
<tr>
<td></td>
<td>(TCP_HIT</td>
</tr>
<tr>
<td></td>
<td>IP</td>
</tr>
<tr>
<td></td>
<td>[(0-9]{1,3}.(0-9]{1,3}.(0-9]{1,3}.(0-9]{1,3}]TCP</td>
</tr>
<tr>
<td></td>
<td>User name</td>
</tr>
<tr>
<td></td>
<td>\s([a-zA-Z0-9]{1,}.)\s+/</td>
</tr>
</tbody>
</table>

Remove Mapping Messages

Remove mapping messages are supported for Blue Coat clients, though no examples are currently available. The following table describes the different known regular expression structure examples used per client for remove mapping messages.

<table>
<thead>
<tr>
<th>Client</th>
<th>Regular expressions</th>
</tr>
</thead>
<tbody>
<tr>
<td>BlueCoat Main Proxy</td>
<td>(TCP_MISS</td>
</tr>
<tr>
<td>BlueCoat Proxy SG</td>
<td>No example currently available.</td>
</tr>
<tr>
<td>BlueCoat Squid Web Proxy</td>
<td>(TCP_MISS</td>
</tr>
</tbody>
</table>

Syslog ISE and ACS Pre-Defined Templates

When listening to ISE or ACS clients, the parser receives the following message types:

- Pass authentication—when the user is authenticated by ISE or ACS, the pass authentication message is issued notifying that authentication succeeded, and including user details. The message is parsed and the user details and session ID are saved from this message.

- Accounting start and accounting update messages (new mapping)—received from ISE or ACS, the accounting start or accounting update message is parsed with the user details and session ID that were saved from the Pass Authentication message and then the user is mapped.

- Accounting stop (remove mapping)—when received from ISE or ACS, the user mapping is deleted from the system.

The supported syslog message format and types for ISE and ACS are as described below.

Pass Authentication Messages

The following messages are supported for Pass Authentication.

- **Header**

  `<181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message`

  For example: `<181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 1 0 message`

- **Body**
Passed-Authentication 000011 10 2016-05-09 12:48:11.011 +03:00 0000012435 5200 NOTICE
Passed-Authentication: Authentication succeeded, ConfigVersionId=104, Device IP Address=10.0.0.12,
DestinationIPAddress=10.0.0.18, DestinationPort=1812, UserA=UserA, Protocol=Radius,
RequestLatency=45, NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA,
NAS-IP-Address=1.1.1.1, Session-Timeout=90, Calling-Station-ID=, cisco-av-pair=audit-session-id=5

• Parsing Example
  User name and session ID only are parsed.
  [UserA,5]

Accounting Start/Update (New Mapping) Messages

The following messages are supported for New Mapping.

• Header
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  For example: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 10 message

• Body
  CISE_RADIUS_Accounting 000011 10 2016-05-09 12:53:52.823 +03:00 0000012451 3000 NOTICE
  Radius-Accounting: RADIUS Accounting start request, ConfigVersionId=104, Device IP
  Address=10.0.0.12, RequestLatency=12, NetworkDeviceName=DefaultNetworkDevice,
  User-Name=UserA, NAS-IP-Address=10.0.0.1, Framed-IP-Address=10.0.0.16, Session-Timeout=90,
  Calling-Station-ID=, Acct-Status-Type=Start, Acct-Session-Id=6, cisco-av-pair=audit-session-id=5

• Parsing Example
  Parsed details include username, and framed IP address, as well as the MAC address if it is included in
  the message.
  [UserA,10.0.0.16]

Remove Mapping Messages

The following messages are supported for Remove Mapping.

• Header
  <181>Sep 13 10:51:41 Server logTag messageId totalFragments currentFragments message
  For example: <181>Sep 13 10:51:41 Positron CISE_PassiveID 0000005255 10 message

• Body
  2016-05-09 12:56:27.274 +03:00 0000012482 3001 NOTICE Radius-Accounting: RADIUS Accounting
  stop request, ConfigVersionId=104, Device IP Address=10.0.0.17, RequestLatency=13,
  NetworkDeviceName=DefaultNetworkDevice, User-Name=UserA, NAS-IP-Address=10.0.0.1,
  Framed-IP-Address=10.0.0.16, Session-Timeout=90, Calling-Station-ID=, Acct-Status-Type=Stop,
  Acct-Session-Id=104, cisco-av-pair=audit-session-id=5

• Parsing Example
  Parsed details include user name, and framed IP address, as well as the MAC address if it is included in
  the message.
Syslog Lucent QIP Pre-Defined Template

The supported syslog message format and types for Lucent QIP are as described below.

**Headers**

Headers supported by the parser are identical for all clients, as described in Work with Syslog Pre-Defined Message Templates, on page 391.

**New Mapping Body Messages**

There are different Lucent QIP body messages that are recognized by the parser as described in the following table.

The regular expression structure for these messages is as follows:

**DHCP_GrantLease** | **DHCP_RenewLease**

Once received, the body is parsed for user details as follows:

{00:0C:29:91:2E:5D,10.0.0.11}

**Body Message**

| DHCP:subtype=0:Single:$IGNORE_N$ DHCP_GrantLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D |
| DHCP:subtype=0:Single:$IGNORE_N$ DHCP_RenewLease: Host=$HOSTNAME$ P=10.0.0.11 MAC=00:0C:29:91:2E:5D |

**Remove Mapping Body Messages**

There are different Lucent QIP body messages that are recognized by the parser as described in the following table.

The regular expression structure for these messages is as follows:

**DeleteLease** | **DHCPAutoRelease**

Once received, the body is parsed for user details as follows:

{10.0.0.11}

**Body Message**

| DHCP:subtype=0:Single:$IGNORE_N$ DeleteLease: IP=10.0.0.11 $IGNORE_N$ |
| DHCP:subtype=0:Single:$IGNORE_N$ DHCPAutoRelease: IP=10.0.0.11 $IGNORE_N$ |

**Filter Passive Identity Services**

You can filter certain users, based on their name or IP address. For example, if you have an administrator from IT services who logs in to an endpoint in order to assist the regular user with that endpoint, you can filter out the administrator activity so it does not appear in Live Sessions, but rather only the regular user of that...
endpoint will appear. The Live Session shows Passive Identity service components that are not filtered out by the Mapping Filters. You can add as many filters as needed. The “OR” logic operator applies between filters. If both the fields are specified in a single filter, the “AND” logic operator applies between these fields.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Work Centres &gt; PassiveID &gt; Providers and then from the left panel choose Mapping Filters.</td>
</tr>
<tr>
<td>2</td>
<td>Choose Providers &gt; Mapping Filters.</td>
</tr>
<tr>
<td>3</td>
<td>Click Add, enter the Username and/or IP address of the user you want to filter and click Submit.</td>
</tr>
<tr>
<td>4</td>
<td>To view the non-filtered users that are currently logged in to the Monitoring session directory, choose Operations &gt; RADIUS Livelog.</td>
</tr>
</tbody>
</table>

**Endpoint Probe**

In addition to the customized providers that you can configure the Endpoint probe is enabled in ISE when the Passive ID service is activated and always runs in the background. The Endpoint probe periodically checks whether each specific user is still logged in to the system.

**Note**

In order to ensure Endpoint runs in the background, you must first configure an initial Active Directory join point and ensure you choose to Store Credentials. For more information about configuring the Endpoint probe, see Work with the Endpoint Probe, on page 404.

To manually check for endpoint status go to Live Sessions, from the Actions column click Show Actions and choose Check current user, as in the following figure.

*Figure 34: Check Current User*

For more information about endpoint user status, and manually running the check, see RADIUS Live Sessions, on page 1156.
When the Endpoint probe recognizes that a user has connected, if 4 hours have passed since the last time the session was updated for the specific endpoint, then it checks whether that user is still logged in and collects the following data:

- MAC address
- Operating system version

Based on the this check, the probe does the following:

- When the user is still logged in, the probe updates ISE with the status Active User.
- When the user has logged out, the session state is updated as Terminated and fifteen minutes later, the user is removed from the Session Directory.
- When the user cannot be contacted, for example, when a firewall prevents contact or the endpoint has shut down, the status is updated as Unreachable and the Subscriber policy will determine how to handle the user session. The endpoint will remain in the Session Directory.

**Work with the Endpoint Probe**

**Before you begin**

Create and enable Endpoint probes based on subnet ranges. One Endpoint probe can be created per PSN. To work with Endpoint probes, first ensure you have configured the following:

- Endpoints must have network connectivity to port 445.
- From ISE, configure an initial Active Directory join point and ensure you select Select Credentials when prompted. For more information about join points, see Active Directory as a Probe and a Provider, on page 362.

**Note**

In order to ensure Endpoint runs in the background, you must first configure an initial Active Directory join point, which enables the Endpoint probe to run even when the Active Directory probe is not fully configured.

**Step 1** Choose Work Centers > Passive ID > Providers and then choose Endpoint Probes.

**Step 2** Click Add to create a new Endpoint probe.

**Step 3** Complete the mandatory fields, ensuring you select Enable from the Status field, and click Submit. See Endpoint Probe Settings, on page 404 for more information.

**Endpoint Probe Settings**

Create a single Endpoint probe per PSN, based on subnet ranges. If you have multiple PSNs in your deployment, then you can allot each PSN for a separate set of subnets, and in so doing, use each probe for a different group of users.
Choose **Work Centers > Passive ID > Providers** and then choose **Endpoint Probes** to configure a new Endpoint Probe for your PSN.

### Table 31: Endpoint Probes Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a unique name by which to identify the use of this probe.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a unique description that explains the use for this probe.</td>
</tr>
<tr>
<td>Status</td>
<td>Choose <strong>Enable</strong> in order to activate this probe.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Choose a PSN for this probe from the list of available PSNs in your deployment.</td>
</tr>
<tr>
<td>Subnets</td>
<td>Enter the subnet range for the group of endpoints that should be checked by this probe. Use standard subnet mask ranges and separate subnet addresses with commas. For example: 10.56.14.111/32,1.1.1.1/24,2.55.2.0/16,2.2.3.0/16,1.2.3.4/32 Each range must be unique and separate from all other ranges. For example, you cannot enter the following ranges for the same probe because they overlap with each other: 2.2.2.0/16,2.2.3.0/16</td>
</tr>
</tbody>
</table>

### Subscribers

The Passive Identity services use Cisco pxGrid services in order to deliver authenticated user identities collected from a variety of providers and stored by the Cisco ISE session directory, to other network systems such as Cisco Stealthwatch or Cisco Firepower Management Center (FMC).

As demonstrated in the following figure, pxGrid is installed on the ISE node, collecting user identities as they are retrieved from external providers, parsed, mapped and so forth. pxGrid then takes those formatted user identities and sends them to Passive Identity service subscribers.
Subscribers connected to Cisco ISE need to register to use the pxGrid services. Subscribers should adopt the pxGrid Client Library available from Cisco through the pxGrid SDK to become the clients. A subscriber can log in to pxGrid using a unique name and certificate-based mutual authentication. Once they have sent a valid certificate, Cisco pxGrid subscribers are automatically approved by ISE.

Subscribers can connect to either a configured pxGrid server host-name or an IP Address. We recommend that you use host name in order to avoid unnecessary errors, particularly in order to ensure the DNS queries work properly. Capabilities are information topics or channels created on pxGrid for subscribers to publish and subscribe. In Cisco ISE, only SessionDirectory and IdentityGroup are supported. Capability information is available from the publisher through publish, directed query, or bulk download query and can be viewed from Subscribers in the Capabilities tab.

To enable subscribers to receive information from ISE, you must:

1. Optionally, generate a certificate from the subscriber's side.
2. Generate pxGrid Certificates for Subscribers, on page 406 from the PassiveID work center.
3. Enable Subscribers, on page 408. You must perform this step, or alternatively automatically enable approvals, in order to allow subscribers to receive user identities from ISE. See Configure Subscriber Settings, on page 408.

You can learn more about Subscribers here:

Generate pxGrid Certificates for Subscribers

Before you begin

You can generate certificates for pxGrid subscribers in order to guarantee mutual trust between pxGrid and the subscribers, thereby enabling user identities to be passed from ISE to the subscribers. To perform the following task, you must be a Super Admin or System Admin.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose Work Centers &gt; PassiveID &gt; Subscribers and go to the Certificates tab.</td>
</tr>
<tr>
<td>2</td>
<td>Select one of the following options from the I want to drop-down list:</td>
</tr>
</tbody>
</table>
• Generate a single certificate without a certificate signing request—You must enter the Common Name (CN) if you select this option. In the Common Name field, enter the pxGrid FQDN which includes pxGrid as the prefix. For example, www.pxgrid-ise.ise.net. Or, alternatively, use wildcards. For example, *.ise.net

• Generate a single certificate with a certificate signing request—You must enter the Certificate Signing Request details if you select this option.

• Generate bulk certificates—You can upload a CSV file that contains the required details.

• Download Root Certificate Chain—download the ISE public root certificates in order to add them to the pxGrid client's trusted certificate store. The ISE pxGrid node only trusts the newly signed pxGrid client certificate and vice-versa, eliminating the need for outside certificate authorities.

Step 3 (optional) You can enter a description for this certificate.

Step 4 View or edit the pxGrid Certificate template on which this certificate is based. Certificate templates contain properties that are common to all certificates issued by the Certificate Authority (CA) based on that template. The certificate template defines the Subject, Subject Alternative Name (SAN), key type, key size, SCEP RA profile that must be used, validity period of the certificate, and the extended key usage (EPU) that specifies whether the certificate has to be used for client or server authentication or both. The internal Cisco ISE CA (ISE CA) uses a certificate template to issue certificates based on that template. To edit this template choose Administration > Certificates > Certificate Authority > Certificate Templates.

Step 5 Specify the Subject Alternative Name (SAN). You can add multiple SANs. The following options are available:

• FQDN—Enter the fully qualified domain name of the ISE node. For example www.isepic.ise.net. Or, alternatively, use wildcards for the FQDN. For example, *.ise.net

An additional line can be added for FQDN in which the pxGrid FQDN can also be entered. This should be identical to the FQDN you used in the Common Name field.

• IP address—Enter the IP address of the ISE node to be associated with the certificate. This information must be entered if the subscriber uses IP addresses instead of an FQDN.

Note This field is not displayed if you have selected the Generate Bulk Certificate option.

Step 6 Select one of the following options from the Certificate Download Format drop-down list:

• Certificate in Private Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)—The root certificate, the intermediate CA certificates, and the end entity certificate are represented in the PEM format. PEM formatted certificate are BASE64-encoded ASCII files. Each certificate starts with the "---------BEGIN CERTIFICATE-----" tag and ends with the "---------END CERTIFICATE-----" tag. The end entity’s private key is stored using PKCS* PEM. It starts with the "-----BEGIN ENCRYPTED PRIVATE KEY-----" tag and ends with the "-----END ENCRYPTED PRIVATE KEY-----" tag.

• PKCS12 format (including certificate chain; one file for both the certificate chain and key)—A binary format to store the root CA certificate, the intermediate CA certificate, and the end entity’s certificate and private key in one encrypted file.

Step 7 Enter a certificate password.

Step 8 Click Create.
Enable Subscribers

You must perform this task, or alternatively automatically enable approvals, in order to allow subscribers to receive user identities from Cisco pxGrid clients. See Configure Subscriber Settings, on page 408.

Before you begin

• Enable the pxGrid persona on at least one node to view the requests from the Cisco pxGrid clients.
• Enable Passive Identity Service. For more information, see Easy Connect, on page 355.

### Step 1
Choose **Work Centers > PassiveID > Subscribers** and ensure you are viewing the **Clients** tab.

### Step 2
Check the checkbox next to the subscriber and click **Approve**.

### Step 3
Click **Refresh** to view the latest status.

View Subscriber Events from Live Logs

The Live Logs page displays all the Subscriber events. Event information includes the subscriber and capability names along with the event type and timestamp.

Navigate to **Subscribers** and select the **Live Log** tab to view the list of events. You can also clear the logs and resynchronize or refresh the list.

Configure Subscriber Settings

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

### Step 1
Choose **Administration > pxGrid Services > Settings**.

### Step 2
Select the following options based on your requirements:

• Automatically Approve New Accounts—Check this checkbox to automatically approve the connection requests from new pxGrid clients.

• Allow Password Based Account Creation—Check this checkbox to enable username/password based authentication for pxGrid clients. If this option is enabled, the pxGrid clients cannot be automatically approved.

A pxGrid client can register itself with the pxGrid controller by sending the username via REST API. The pxGrid controller generates a password for the pxGrid client during client registration. The administrator can approve or deny the connection request.

### Step 3
Click **Save**.
Monitoring and Troubleshooting Service in PassiveID Work Center

Learn about how you can manage PassiveID Work Center with monitoring, troubleshooting and reporting tools.

- RADIUS Live Sessions, on page 1156
- Cisco ISE Alarms, on page 862
- Reports, on page 905
- TCP Dump Utility to Validate the Incoming Traffic, on page 892

LDAP

Lightweight Directory Access Protocol (LDAP) is a networking protocol defined by RFC 2251 for querying and modifying directory services that run on TCP/IP. LDAP is a lightweight mechanism for accessing an X.500-based directory server.

Cisco ISE integrates with an LDAP external database, which is also called an identity source, by using the LDAP protocol.

LDAP Directory Service

LDAP directory service is based on a client-server model. A client starts an LDAP session by connecting to an LDAP server and sending operation requests to the server. The server then sends its responses. One or more LDAP servers contain data from the LDAP directory tree or the LDAP backend database.

The directory service manages a directory, which is a database that holds information. Directory services use a distributed model for storing information, and that information is usually replicated between directory servers.

An LDAP directory is organized in a simple tree hierarchy and can be distributed among many servers. Each server can have a replicated version of the total directory, which is synchronized periodically.

An entry in the tree contains a set of attributes, where each attribute has a name (an attribute type or attribute description) and one or more values. The attributes are defined in a schema.

Each entry has a unique identifier: its distinguished name (DN). This name contains the relative distinguished name (RDN), which is constructed from attributes in the entry, followed by the DN of the parent entry. You can think of the DN as a full filename, and the RDN as a relative filename in a folder.

Multiple LDAP Instances

By creating more than one LDAP instance with different IP addresses or port settings, you can configure Cisco ISE to authenticate using different LDAP servers or different databases on the same LDAP server. Each primary server IP address and port configuration, along with the secondary server IP address and port configuration, forms an LDAP instance that corresponds to one Cisco ISE LDAP identity source instance.

Cisco ISE does not require that each LDAP instance correspond to a unique LDAP database. You can have more than one LDAP instance set to access the same database. This method is useful when your LDAP database contains more than one subtree for users or groups. Because each LDAP instance supports only one subtree directory for users and one subtree directory for groups, you must configure separate LDAP instances.
for each user directory and group directory subtree combination for which Cisco ISE submits authentication requests.

**LDAP Failover**

Cisco ISE supports failover between a primary LDAP server and a secondary LDAP server. A failover occurs when an authentication request fails because Cisco ISE could not connect to an LDAP server because it is down or is otherwise unreachable.

If you establish failover settings and the first LDAP server that Cisco ISE attempts to contact cannot be reached, Cisco ISE always attempts to contact a second LDAP server. If you want Cisco ISE to use the first LDAP server again, you must enter a value in the Failback Retry Delay text box.

---

**Note**

Cisco ISE always uses the primary LDAP server to obtain groups and attributes for use in authorization policies from the Admin portal, so the primary LDAP server must be accessible when you configure these items. Cisco ISE uses the secondary LDAP server only for authentications and authorizations at run time, according to the failover configuration.

**LDAP Connection Management**

Cisco ISE supports multiple concurrent LDAP connections. Connections are opened on demand at the time of the first LDAP authentication. The maximum number of connections is configured for each LDAP server. Opening connections in advance shortens the authentication time. You can set the maximum number of connections to use for concurrent binding connections. The number of open connections can be different for each LDAP server (primary or secondary) and is determined based on the maximum number of administration connections configured for each server.

Cisco ISE retains a list of open LDAP connections (including the binding information) for each LDAP server that is configured in Cisco ISE. During the authentication process, the connection manager attempts to find an open connection from the pool. If an open connection does not exist, a new one is opened.

If the LDAP server closed the connection, the connection manager reports an error during the first call to search the directory, and tries to renew the connection. After the authentication process is complete, the connection manager releases the connection.

**LDAP User Authentication**

LDAP can be used as an external database for Cisco ISE user authentication. Cisco ISE supports plain password authentication. User authentication includes:

- Searching the LDAP server for an entry that matches the username in the request
- Checking the user password with the one that is found in the LDAP server
- Retrieving a group’s membership information for use in policies
- Retrieving values for specified attributes for use in policies and authorization profiles
To authenticate a user, Cisco ISE sends a bind request to the LDAP server. The bind request contains the DN and password of the user in clear text. A user is authenticated when the DN and password of the user match the username and password in the LDAP directory.

We recommend that you protect the connection to the LDAP server using Secure Sockets Layer (SSL).

Note

Change Password option is supported for LDAP only if there are remaining grace logins for the account after the password has expired. The LDAP server's bindResponse should be LDAP_SUCCESS, and should include the remaining grace logins control field in the bindResponse message. If the bindResponse message contains any additional control field (other than remaining grace logins), it might result in decoding error in ISE.

LDAP Group and Attribute Retrieval for Use in Authorization Policies

Cisco ISE can authenticate a subject (user or host) against an LDAP identity source by performing a bind operation on the directory server to find and authenticate the subject. After successful authentication, Cisco ISE can retrieve groups and attributes that belong to the subject whenever they are required. You can configure the attributes to be retrieved in the Cisco ISE Admin portal by choosing Administration > Identity Management > External Identity Sources > LDAP. These groups and attributes can be used by Cisco ISE to authorize the subject.

To authenticate a user or query the LDAP identity source, Cisco ISE connects to the LDAP server and maintains a connection pool.

You should note the following restrictions on group memberships when Active Directory is configured as an LDAP store:

• Users or computers must be direct members of the group defined in the policy conditions to match the policy rule.

• The defined group may not be a user’s or computer’s primary group. This restriction is applicable only when Active Directory is configured as an LDAP store.

LDAP Group Membership Information Retrieval

For user authentication, user lookup, and MAC address lookup, Cisco ISE must retrieve group membership information from LDAP databases. LDAP servers represent the association between a subject (a user or a host) and a group in one of the following ways:

• Groups Refer to Subjects—The group objects contain an attribute that specifies the subject. Identifiers for subjects can be sourced in the group as the following:

  • Distinguished names
  • Plain usernames

• Subjects Refer to Groups—The subject objects contain an attribute that specifies the group to which they belong.

LDAP identity sources contain the following parameters for group membership information retrieval:

• Reference direction—This parameter specifies the method to use when determining group membership (either groups to subjects or subjects to groups).
• Group map attribute—This parameter indicates the attribute that contains group membership information.
• Group object class—This parameter determines that certain objects are recognized as groups.
• Group search subtree—This parameter indicates the search base for group searches.
• Member type option—This parameter specifies how members are stored in the group member attribute (either as DNs or plain usernames).

LDAP Attributes Retrieval

For user authentication, user lookup, and MAC address lookup, Cisco ISE must retrieve the subject attributes from LDAP databases. For each instance of an LDAP identity source, an identity source dictionary is created. These dictionaries support attributes of the following data types:
• String
• Unsigned integer 32
• IPv4 address

For unsigned integers and IPv4 attributes, Cisco ISE converts the strings that it has retrieved to the corresponding data types. If conversion fails or if no values are retrieved for the attributes, Cisco ISE logs a debug message, but the authentication or lookup process does not fail.

You can optionally configure default values for the attributes that Cisco ISE can use when the conversion fails or when Cisco ISE does not retrieve any values for the attributes.

LDAP Certificate Retrieval

If you have configured certificate retrieval as part of user lookup, then Cisco ISE must retrieve the value of the certificate attribute from LDAP. To retrieve the value of the certificate attribute from LDAP, you must have previously configured the certificate attribute in the list of attributes to be accessed while configuring an LDAP identity source.

Errors Returned by the LDAP Server

The following errors can occur during the authentication process:
• Authentication Errors—Cisco ISE logs authentication errors in the Cisco ISE log files.

Possible reasons for an LDAP server to return binding (authentication) errors include the following:
• Parameter errors—Invalid parameters were entered
• User account is restricted (disabled, locked out, expired, password expired, and so on)
• Initialization Errors—Use the LDAP server timeout settings to configure the number of seconds that Cisco ISE should wait for a response from an LDAP server before determining that the connection or authentication on that server has failed.

Possible reasons for an LDAP server to return an initialization error are:
• LDAP is not supported.
• The server is down.
• The server is out of memory.
• The user has no privileges.
• Administrator credentials are configured incorrectly.

The following errors are logged as external resource errors, indicating a possible problem with the LDAP server:
• A connection error occurred
• The timeout expired
• The server is down
• The server is out of memory

The following error is logged as an Unknown User error:
• A user does not exist in the database

The following error is logged as an Invalid Password error, where the user exists, but the password sent is invalid:
• An invalid password was entered

**LDAP User Lookup**

Cisco ISE supports the user lookup feature with an LDAP server. This feature allows you to search for a user in the LDAP database and retrieve information without authentication. The user lookup process includes the following actions:
• Searching the LDAP server for an entry that matches the username in the request
• Retrieving a user’s group membership information for use in policies
• Retrieving values for specified attributes for use in policies and authorization profiles

**LDAP MAC Address Lookup**

Cisco ISE supports the MAC address lookup feature. This feature allows you to search for a MAC address in the LDAP database and retrieve information without authentication. The MAC address lookup process includes the following actions:
• Searching the LDAP server for an entry that matches the MAC address of the device
• Retrieving a MAC Address group information for the device for use in policies
• Retrieving values for specified attributes for use in policies
Add LDAP Identity Sources

Before you begin

• To perform the following task, you must be a Super Admin or System Admin.

• Cisco ISE always uses the primary LDAP server to obtain groups and attributes for use in authorization policies. Therefore, your primary LDAP server must be reachable when you configure these items.

Step 1: Choose Administration > Identity Management > External Identity Sources > LDAP > Add.
Step 2: Enter the values.
Step 3: Click Submit to create an LDAP instance.

Related Topics

LDAP, on page 409
LDAP Directory Service, on page 409
Multiple LDAP Instances, on page 409
LDAP Failover, on page 410
LDAP Connection Management, on page 410
LDAP User Authentication, on page 410
LDAP Group and Attribute Retrieval for Use in Authorization Policies, on page 411
LDAP Group Membership Information Retrieval, on page 411
LDAP Attributes Retrieval, on page 412
LDAP Certificate Retrieval, on page 412
Errors Returned by the LDAP Server, on page 412
LDAP User Lookup, on page 413
LDAP MAC Address Lookup, on page 413
Configure Primary and Secondary LDAP Servers, on page 415
Enable Cisco ISE to Obtain Attributes from the LDAP Server, on page 415
Retrieve Group Membership Details from the LDAP Server, on page 415
Retrieve User Attributes From the LDAP Server, on page 416
Enable Secure Authentication with LDAP Identity Source, on page 416

Configure LDAP Schema

Step 1: Choose Administration > Identity Management > External Identity Sources > LDAP.
Step 2: Select the LDAP instance.
Step 3: Click the General tab.
Step 4: Click the drop-down arrow near the Schema option.
Step 5: Select the required schema from the Schema drop-down list. You can select the Custom option to update the attributes based on your requirements.
Predefined attributes are used for the built-in schema, such as Active Directory, Sun directory Server, Novell eDirectory. If you edit the attributes of the predefined schema, Cisco ISE automatically creates a custom schema.

**Configure Primary and Secondary LDAP Servers**

After you create an LDAP instance, you must configure the connection settings for the primary LDAP server. Configuring a secondary LDAP server is optional.

**Step 1** Choose Administration > Identity Management > External Identity Sources > LDAP.

**Step 2** Check the check box next to the LDAP instance that you want to edit and click Edit.

**Step 3** Click the Connection tab to configure the primary and secondary servers.

**Step 4** Enter the values as described in LDAP Identity Source Settings.

**Step 5** Click Submit to save the connection parameters.

**Enable Cisco ISE to Obtain Attributes from the LDAP Server**

For Cisco ISE to obtain user and group data from an LDAP server, you must configure LDAP directory details in Cisco ISE. For LDAP identity source, the following three searches are applicable:

- Search for all groups in group subtree for administration
- Search for user in subject subtree to locate user
- Search for groups in which the user is a member

**Step 1** Choose Administration > Identity Management > External Identity Sources > LDAP.

**Step 2** Check the check box next to the LDAP instance that you want to edit and click Edit.

**Step 3** Click the Directory Organization tab.

**Step 4** Enter the values as described in LDAP Identity Source Settings.

**Step 5** Click Submit to save the configuration.

**Retrieve Group Membership Details from the LDAP Server**

You can add new groups or select groups from the LDAP directory.

**Step 1** Choose Administration > Identity Management > External Identity Sources > LDAP.

**Step 2** Check the check box next to the LDAP instance that you want to edit and click Edit.

**Step 3** Click the Groups tab.

**Step 4** Choose Add > Add Group to add a new group or choose Add > Select Groups From Directory to select the groups from the LDAP directory.

a) If you choose to add a group, enter a name for the new group.
b) If you are selecting from the directory, enter the filter criteria, and click **Retrieve Groups**. Your search criteria can contain the asterisk (*) wildcard character.

**Step 5**
Check the check boxes next to the groups that you want to select and click **OK**.
The groups that you have selected will appear in the Groups page.

**Step 6**
Click **Submit** to save the group selection.

---

**Note**
Active Directory built-in groups are not supported when Active Directory is configured as LDAP Identity Store in Cisco ISE.

---

**Retrieve User Attributes From the LDAP Server**
You can obtain user attributes from the LDAP server for use in authorization policies.

**Step 1**
Choose **Administration** > **Identity Management** > **External Identity Sources** > **LDAP**.

**Step 2**
Check the check box next to the LDAP instance that you want to edit and click **Edit**.

**Step 3**
Click the **Attributes** tab.

**Step 4**
Choose **Add** > **Add Attribute** to add a new attribute or choose **Add** > **Select Attributes From Directory** to select attributes from the LDAP server.

a) If you choose to add an attribute, enter a name for the new attribute.
b) If you are selecting from the directory, enter an example user and click **Retrieve Attributes** to retrieve the user’s attributes. You can use the asterisk (*) wildcard character.

Cisco ISE allows you to configure the LDAP server with IPv4 or IPv6 address for user authentication when you manually add the attribute type IP.

**Step 5**
Check the check boxes next to the attributes that you want to select, then click **OK**.

**Step 6**
Click **Submit** to save the attribute selections.

---

**Enable Secure Authentication with LDAP Identity Source**
When you choose the Secure Authentication option in the LDAP configuration page, Cisco ISE uses SSL to secure communication with the LDAP identity source. Secure connection to LDAP identity source is established using:

- **SSL tunnel**—Using SSL v3 or TLS v1 (the strongest version supported by the LDAP server)
- **Server authentication** (authentication of LDAP server)—Certificate based
- **Client authentication** (authentication of Cisco ISE)—None (Administrator bind is used inside the SSL tunnel)
- **Cipher suites**—All cipher suites supported by Cisco ISE

We recommend that you use TLS v1 with the strongest encryption and ciphers that Cisco ISE supports.
To enable Cisco ISE to communicate securely with the LDAP identity source:

**Before you begin**
- Cisco ISE must be connected to an LDAP server
- TCP port 636 should be open

**Step 1** Import the full Certificate Authority (CA) chain of the CA that issued the server certificate to the LDAP server into Cisco ISE (Administration > System > Certificates > Trusted Certificates).

The full CA chain refers to the root CA and intermediate CA certificates; not the LDAP server certificate.

**Step 2** Configure Cisco ISE to use secure authentication when communicating with the LDAP identity source (Administration > Identity Management > External Identity Sources > LDAP; be sure to check the Secure Authentication check box in the Connection Setting tab).

**Step 3** Select the root CA certificate in the LDAP identity store.

**ODBC Identity Source**

You can use an Open Database Connectivity (ODBC)-compliant database as an external identity source to authenticate users and endpoints. ODBC identity source can be used in an identity store sequence and for Guest and Sponsor authentications. It can also be used for BYOD flow.

The following database engines are supported:
- MySQL
- Oracle
- PostgreSQL
- Microsoft SQL Server
- Sybase

Configuring Cisco ISE to authenticate against an ODBC-compliant database does not affect the configuration of the database. To manage your database, refer to your database documentation.

**Credential Check for ODBC Database**

Cisco ISE supports three different types of credential check for an ODBC database. You must configure appropriate SQL stored procedure for each credential check type. uses the stored procedure to query the appropriate tables in the ODBC database and receive the output parameters and/or recordset from ODBC database. The database can return a recordset or a set of named parameters in response to an ODBC query.

The password can be stored in an ODBC database in clear text or encrypted format. The stored procedure can decrypt it back to clear text when it is called by Cisco ISE.
<table>
<thead>
<tr>
<th>Credential Check Type</th>
<th>ODBC Input Parameters</th>
<th>ODBC Output Parameters</th>
<th>Credential Check</th>
<th>Authentication Protocols</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain text password authentication in ODBC database</td>
<td>Username Password</td>
<td>Result Group Account Info Error string</td>
<td>If the username and password are matched, relevant user information is returned.</td>
<td>PAP EAP-GTC (as inner method of PEAP or EAP-FAST) TACACS</td>
</tr>
<tr>
<td>Plain text password fetching from ODBC database</td>
<td>Username</td>
<td>Result Group Account Info Error string Password</td>
<td>If the username is found, its password and relevant user information is returned by the stored procedure. Cisco ISE calculates the password hash based on the authentication method and compares it with the one received from the client.</td>
<td>CHAP MSCHAPv1/v2 EAP-MD5 LEAP EAP-MSCHAPv2 (as inner method of PEAP or EAP-FAST) TACACS</td>
</tr>
<tr>
<td>Lookup</td>
<td>Username</td>
<td>Result Group Account Info Error string</td>
<td>If the username is found, relevant user information is returned.</td>
<td>MAB Fast reconnect of PEAP, EAP-FAST, and EAP-TTLS</td>
</tr>
</tbody>
</table>

**Note:** The groups that are returned in the output parameters are not used in Cisco ISE. Only the groups that are retrieved by the Fetch Groups stored procedure are used in Cisco ISE. The account info is included only in the authentication audit log.
The following table lists the mapping between the result codes returned by the ODBC database stored procedure and Cisco ISE authentication result codes:

<table>
<thead>
<tr>
<th>Result code (returned by the stored procedure)</th>
<th>Description</th>
<th>Cisco ISE authentication result code</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>CODE_SUCCESS</td>
<td>NA (authentication passed)</td>
</tr>
<tr>
<td>1</td>
<td>CODE_UNKNOWN_USER</td>
<td>UnknownUser</td>
</tr>
<tr>
<td>2</td>
<td>CODE_INVALID_PASSWORD</td>
<td>Failed</td>
</tr>
<tr>
<td>3</td>
<td>CODE_UNKNOWN_USER_OR_INVALID_PASSWORD</td>
<td>UnknownUser</td>
</tr>
<tr>
<td>4</td>
<td>CODE_INTERNAL_ERROR</td>
<td>Error</td>
</tr>
<tr>
<td>10001</td>
<td>CODE_ACCOUNT_DISABLED</td>
<td>DisabledUser</td>
</tr>
<tr>
<td>10002</td>
<td>CODE_PASSWORD_EXPIRED</td>
<td>NotPerformedPasswordExpired</td>
</tr>
</tbody>
</table>

Cisco ISE performs the actual authentication/lookup operation based on this mapped authentication result code.

You can use the stored procedures to fetch groups and attributes from the ODBC database.

**Sample procedure that returns recordset for plain text password authentication (for Microsoft SQL Server)**

```sql
CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsRecordset]
    @username varchar(64), @password varchar(255)
AS
BEGIN
    IF EXISTS( SELECT username
        FROM NetworkUsers
        WHERE username = @username
        AND password = @password )
        SELECT 0,11,'give full access','No Error'
        FROM NetworkUsers
        WHERE username = @username
    ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```

**Sample procedure that returns recordset for plain text password fetching (for Microsoft SQL Server)**

```sql
CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsRecordset]
    @username varchar(64)
AS
BEGIN
    IF EXISTS( SELECT username
        FROM NetworkUsers
        WHERE username = @username)
        SELECT 0,11,'give full access','No Error',password
        FROM NetworkUsers
        WHERE username = @username
    ELSE
        SELECT 3,0,'odbc','ODBC Authen Error'
END
```
ELSE
  SELECT 3,0,'odbc','ODBC Authen Error'
END

Sample procedure that returns recordset for Lookup (for Microsoft SQL Server)

CREATE PROCEDURE [dbo].[ISEUserLookupReturnsRecordset]
  @username varchar(64)
AS
BEGIN
  IF EXISTS( SELECT username
  FROM NetworkUsers
  WHERE username = @username)
  SELECT 0,11,'give full access','No Error'
  FROM NetworkUsers
  WHERE username = @username
ELSE
  SELECT 3,0,'odbc','ODBC Authen Error'
END

Sample procedure that returns parameters for plain text password authentication (for Microsoft SQL Server)

CREATE PROCEDURE [dbo].[ISEAuthUserPlainReturnsParameters]
  @username varchar(64), @password varchar(255), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
  IF EXISTS( SELECT username
  FROM NetworkUsers
  WHERE username = @username
  AND password = @password )
  SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error'
  FROM NetworkUsers
  WHERE username = @username
ELSE
  SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END

Sample procedure that returns parameters for plain text password fetching (for Microsoft SQL Server)

CREATE PROCEDURE [dbo].[ISEFetchPasswordReturnsParameters]
  @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo varchar(255) OUTPUT, @errorString varchar(255) OUTPUT, @password varchar(255) OUTPUT
AS
BEGIN
  IF EXISTS( SELECT username
  FROM NetworkUsers
  WHERE username = @username)
  SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error',
  @password=password
  FROM NetworkUsers
  WHERE username = @username
ELSE
  SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END

Sample procedure that returns parameters for Lookup (for Microsoft SQL Server)

CREATE PROCEDURE [dbo].[ISEUserLookupReturnsParameters]
  @username varchar(64), @result INT OUTPUT, @group varchar(255) OUTPUT, @acctInfo varchar(255) OUTPUT, @errorString varchar(255) OUTPUT
AS
BEGIN
IF EXISTS( SELECT username
FROM NetworkUsers
WHERE username = @username)
SELECT @result=0, @group=11, @acctInfo='give full access', @errorString='No Error'
FROM NetworkUsers
WHERE username = @username
ELSE
SELECT @result=3, @group=0, @acctInfo='odbc', @errorString='ODBC Authen Error'
END

Sample procedure that fetches groups from Microsoft SQL Server

CREATE PROCEDURE [dbo].[ISEGroupsH]
@username varchar(64), @result int output
AS
BEGIN
  if exists (select * from NetworkUsers where username = @username)
  begin
    set @result = 0
    select 'accountants', 'engineers', 'sales','test_group2'
  end
  else
  set @result = 1
END

Sample procedure that fetches all the groups of all the users if the username is "*" (for Microsoft SQL Server)

ALTER PROCEDURE [dbo].[ISEGroupsH]
@username varchar(64), @result int output
AS
BEGIN
  if @username = '*'
  begin
    -- if username is equal to '*' then return all existing
    groups
    set @result = 0
    select 'accountants', 'engineers',
    'sales','test_group1','test_group2','test_group3','test_group4'
  end
  else
  if exists (select * from NetworkUsers where username = @username)
  begin
    set @result = 0
    select 'accountants'
  end
  else
  set @result = 1
END

Sample procedure that fetches attributes from Microsoft SQL Server

CREATE PROCEDURE [dbo].[ISEAttrsH]
@username varchar(64), @result int output
AS
BEGIN
  if exists (select * from NetworkUsers where username = @username)
  begin
    set @result = 0
    select phone as phone, username as username, department as
    department, floor as floor, memberOf as memberOf, isManager as isManager from NetworkUsers
    where username = @username
  end
  else

Add ODBC Identity Source

Before you begin
To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose Administration > Identity Management > External Identity Sources.
Step 2 Click ODBC.
Step 3 Click Add.
Step 4 In the General tab, enter a name and description for the ODBC identity source.
Step 5 In the Connection tab, enter the following details:
   • Hostname or IP address of the ODBC database (If a non-standard TCP port is used for the database, you can specify the port number in the following format: hostname or IP address:port)
   • Name of the ODBC database
   • Admin username and password (Cisco ISE connects to the database using these credentials)
   • Server timeout in seconds (default is 5 seconds)
   • Connection attempts (default is 1)
   • Select the database type. Choose one of the following:
     • MySQL
     • Oracle
     • PostgreSQL
     • Microsoft SQL Server
     • Sybase

Step 6 Click Test Connection to check the connectivity with the ODBC database and to verify the existence of the stored procedures for the configured use cases.
Step 7 In the Stored Procedures tab, enter the following details:
   • Stored Procedure Type—Select the type of output that your database provides:
     • Returns Recordset—The database returns a recordset in response to an ODBC query.
     • Returns Parameters—The database returns a set of named parameters in response to an ODBC query.

   • Plain Text Password Authentication—Enter the name of the stored procedure that runs on the ODBC server for plain text password authentication. Used for PAP, EAP-GTC inner method, and TACACS.

   • Plain Text Password Fetching—Enter the name of the stored procedure that runs on the ODBC server for plain text password fetching. Used for CHAP, MS-CHAPv1/v2, LEAP, EAP-MD5, EAP-MSCHAPv2 inner method, and TACACS.
• Check username or machine exists—Enter the name of the stored procedure that runs on the ODBC server for User/MAC address lookup. Used for MAB and fast reconnect of PEAP, EAP-FAST, and EAP-TTLS.
• Fetch Groups—Enter the name of the stored procedure that retrieves the groups from the ODBC database.
• Fetch Attributes—Enter the name of the stored procedure that retrieves the attributes and their values from the ODBC database.
• Search for MAC address in format—The incoming MAC address is normalized based on the selected MAC format.

**Step 8**
Add the required attributes in the **Attributes** tab. While adding an attribute, you can specify how the attribute name should appear in the authorization policy rules.

You can also fetch the attributes from the ODBC database. You can retrieve the attributes from the ODBC database by using both the username and MAC address. String, boolean, and integer attributes are supported. These attributes can be used in the authorization policies.

**Step 9**
Add the user groups in the **Groups** tab. You can also fetch the groups from the ODBC database by specifying the username or MAC address. These groups can be used in the authorization policies.

You can rename the groups and attributes. By default, the name that is displayed in the "Name in ISE" field is same as that in ODBC database, however, you can modify this name. This name is used in the authorization policies.

**Step 10**
Click **Submit**.

---

**RADIUS Token Identity Sources**

A server that supports the RADIUS protocol and provides authentication, authorization, and accounting (AAA) services to users and devices is called a RADIUS server. A RADIUS identity source is simply an external identity source that contains a collection of subjects and their credentials and uses the RADIUS protocol for communication. For example, the Safeword token server is an identity source that can contain several users and their credentials as one-time passwords that provides an interface that you can query using the RADIUS protocol.

Cisco ISE supports any RADIUS RFC 2865-compliant server as an external identity source. Cisco ISE supports multiple RADIUS token server identities, for example the RSA SecurID server and the SafeWord server. RADIUS identity sources can work with any RADIUS token server that is used to authenticate a user.

---

**Note**

The Process Host Lookup option must be enabled for MAB authentication. We recommend that you don’t configure the RADIUS token server that is used as the external identity source, for MAB authentication, because the devices that are using MAB authentication cannot generate an OTP or a RADIUS token (which is required for RADIUS token server authentication). Hence, the authentication will fail. You can use the external RADIUS server option to process the MAB requests.

---

**RADIUS Token Server Supported Authentication Protocols**

Cisco ISE supports the following authentication protocols for RADIUS identity sources:

• RADIUS PAP
- Protected Extensible Authentication Protocol (PEAP) with inner Extensible Authentication Protocol-Generic Token Card (EAP-GTC)
- EAP-FAST with inner EAP-GTC

Ports Used By the RADIUS Token Servers for Communication

RADIUS token servers use the UDP port for authentication sessions. This port is used for all RADIUS communication. For Cisco ISE to send RADIUS one-time password (OTP) messages to a RADIUS-enabled token server, you must ensure that the gateway devices between Cisco ISE and the RADIUS-enabled token server allow communication over the UDP port. You can configure the UDP port through the Admin portal.

RADIUS Shared Secret

You must provide a shared secret while configuring RADIUS identity sources in Cisco ISE. This shared secret should be the same as the shared secret that is configured on the RADIUS token server.

Failover in RADIUS Token Servers

Cisco ISE allows you to configure multiple RADIUS identity sources. Each RADIUS identity source can have primary and secondary RADIUS servers. When Cisco ISE is unable to connect to the primary server, it uses the secondary server.

Configurable Password Prompt in RADIUS Token Servers

RADIUS identity sources allow you to configure the password prompt. You can configure the password prompt through the Admin portal.

RADIUS Token Server User Authentication

Cisco ISE obtains the user credentials (username and passcode) and passes them to the RADIUS token server. Cisco ISE also relays the results of the RADIUS token server authentication processing to the user.

User Attribute Cache in RADIUS Token Servers

RADIUS token servers, by default, do not support user lookups. However, the user lookup functionality is essential for the following Cisco ISE features:

- PEAP session resume—This feature allows the PEAP session to resume after successful authentication during EAP session establishment.
- EAP/FAST fast reconnect—This feature allows fast reconnection after successful authentication during EAP session establishment.

Cisco ISE caches the results of successful authentications to process user lookup requests for these features. For every successful authentication, the name of the authenticated user and the retrieved attributes are cached. Failed authentications are not written to the cache.
The cache is available in the memory at runtime and is not replicated between Cisco ISE nodes in a distributed deployment. You can configure the Time to Live (TTL) limit for the cache through the Admin portal. You must enable the identity caching option and set the aging time in minutes. The cache is available in the memory for the specified amount of time.

**RADIUS Identity Source in Identity Sequence**

You can add the RADIUS identity source for authentication sequence in an identity source sequence. However, you cannot add the RADIUS identity source for attribute retrieval sequence because you cannot query the RADIUS identity source without authentication. Cisco ISE cannot distinguish among different errors while authenticating with a RADIUS server. RADIUS servers return an Access-Reject message for all errors. For example, when a user is not found in the RADIUS server, instead of returning a User Unknown status, the RADIUS server returns an Access-Reject message.

**RADIUS Server Returns the Same Message for All Errors**

When a user is not found in the RADIUS server, the RADIUS server returns an Access-Reject message. Cisco ISE provides an option to configure this message through the Admin portal as either an Authentication Failed or a User Not Found message. However, this option returns a User Not Found message not only for cases where the user is not known, but for all failure cases.

The following table lists the different failure cases that are possible with RADIUS identity servers.

*Table 32: Error Handling*

<table>
<thead>
<tr>
<th>Failure Cases</th>
<th>Reasons for Failure</th>
</tr>
</thead>
</table>
| Authentication Failed | • User is unknown.  
  • User attempts to log in with an incorrect passcode.  
  • User login hours expired. |
| Process Failed   | • RADIUS server is configured incorrectly in Cisco ISE.  
  • RADIUS server is unavailable.  
  • RADIUS packet is detected as malformed.  
  • Problem during sending or receiving a packet from the RADIUS server.  
  • Timeout. |
| Unknown User     | Authentication failed and the Fail on Reject option is set to false. |

**Safeword Server Supports Special Username Format**

The Safeword token server supports authentication with the following username format:
Username—Username, OTP

As soon as Cisco ISE receives the authentication request, it parses the username and converts it to the following username:

Username—Username

The SafeWord token servers support both of these formats. Cisco ISE works with various token servers. While configuring a SafeWord server, you must check the SafeWord Server check box in the Admin portal for Cisco ISE to parse the username and convert it to the specified format. This conversion is done in the RADIUS token server identity source before the request is sent to the RADIUS token server.

Authentication Request and Response in RADIUS Token Servers

When Cisco ISE forwards an authentication request to a RADIUS-enabled token server, the RADIUS authentication request contains the following attributes:

- User-Name (RADIUS attribute 1)
- User-Password (RADIUS attribute 2)
- NAS-IP-Address (RADIUS attribute 4)

Cisco ISE expects to receive any one of the following responses:

- Access-Accept—No attributes are required, however, the response can contain a variety of attributes based on the RADIUS token server configuration.
- Access-Reject—No attributes are required.
- Access-Challenge—The attributes that are required per RADIUS RFC are the following:
  - State (RADIUS attribute 24)
  - Reply-Message (RADIUS attribute 18)
  - One or more of the following attributes: Vendor-Specific, Idle-Timeout (RADIUS attribute 28), Session-Timeout (RADIUS attribute 27), Proxy-State (RADIUS attribute 33)

  No other attributes are allowed in Access-Challenge.

Add a RADIUS Token Server

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1
Choose Administration > Identity Management > External Identity Sources > RADIUS Token > Add.

Step 2
Enter the values in the General and Connection tabs.

Step 3
Click the Authentication tab.

This tab allows you to control the responses to an Access-Reject message from the RADIUS token server. This response could either mean that the credentials are invalid or that the user is not known. Cisco ISE accepts one of the following
responses: Failed authentication or User not found. This tab also allows you to enable identity caching and to set the aging time for the cache. You can also configure a prompt to request the password.

a) Click the Treat Rejects as ‘authentication failed’ radio button if you want the Access-Reject response from the RADIUS token server to be treated as a failed authentication.

b) Click the Treat Rejects as ‘user not found’ radio button if you want the Access-Reject response from the RADIUS token server to be treated as an unknown user failure.

**Step 4**

Check the Enable Passcode Caching check box if you want Cisco ISE to store the passcode in the cache after the first successful authentication with an RADIUS token server and use the cached user credentials for the subsequent authentications if they happen within the configured time period.

Enter the number of seconds for which the passcode must be stored in the cache in the Aging Time field. Within this period of time, the user can perform more than one authentication with the same passcode. The default value is 30 seconds. The valid range is from 1 to 300 seconds.

**Note**
Cisco ISE clears the cache after the first failed authentication. The user must enter a new, valid passcode.

**Note**
We strongly recommend that you enable this option only when you use a protocol that supports encryption of the passcode, for example, EAP-FAST-GTC. For information on supported authentication protocols for RADIUS Token server, see RADIUS Token Server Supported Authentication Protocols, on page 423

**Step 5**

Click the Authorization tab.

This tab allows you to configure a name that will appear for the attribute that is returned by the RADIUS token server while sending an Access-Accept response to Cisco ISE. This attribute can be used in authorization policy conditions. The default value is CiscoSecure-Group-Id.

**Step 6**

Click Submit.

### Related Topics

- RADIUS Token Identity Sources, on page 423
- RADIUS Token Server Supported Authentication Protocols, on page 423
- Ports Used By the RADIUS Token Servers for Communication, on page 424
- RADIUS Shared Secret, on page 424
- Failover in RADIUS Token Servers, on page 424
- Configurable Password Prompt in RADIUS Token Servers, on page 424
- RADIUS Token Server User Authentication, on page 424
- User Attribute Cache in RADIUS Token Servers, on page 424
- RADIUS Identity Source in Identity Sequence, on page 425
- RADIUS Server Returns the Same Message for All Errors, on page 425
- Safeword Server Supports Special Username Format, on page 425
- Authentication Request and Response in RADIUS Token Servers, on page 426

### Delete a RADIUS Token Server

**Before you begin**

- To perform the following task, you must be a Super Admin or System Admin.
• Ensure that you do not select the RADIUS token servers that are part of an identity source sequence. If you select a RADIUS token server that is part of an identity source sequence for deletion, the delete operation fails.

**Step 1**  Choose Administration > Identity Management > External Identity Sources > RADIUS Token.

**Step 2**  Check the check box next to the RADIUS token server or servers that you want to delete, then click Delete.

**Step 3**  Click OK to delete the RADIUS token server or servers that you have selected.

If you select multiple RADIUS token servers for deleting, and one of them is used in an identity source sequence, the delete operation fails and none of the RADIUS token servers are deleted.

---

**RSA Identity Sources**

Cisco ISE supports the RSA SecurID server as an external database. RSA SecurID two-factor authentication consists of the PIN of the user and an individually registered RSA SecurID token that generates single-use token codes based on a time code algorithm. A different token code is generated at fixed intervals (usually each at 30 or 60 seconds). The RSA SecurID server validates this dynamic authentication code. Each RSA SecurID token is unique, and it is not possible to predict the value of a future token based on past tokens. Thus, when a correct token code is supplied together with a PIN, there is a high degree of certainty that the person is a valid user. Therefore, RSA SecurID servers provide a more reliable authentication mechanism than conventional reusable passwords.

Cisco ISE supports the following RSA identity sources:

- RSA ACE/Server 6.x series
- RSA Authentication Manager 7.x and 8.0 series

You can integrate with RSA SecurID authentication technology in any one of the following ways:

- Using the RSA SecurID agent—Users are authenticated with their username and passcode through the RSA native protocol.
- Using the RADIUS protocol—Users are authenticated with their username and passcode through the RADIUS protocol.

The RSA SecurID token server in Cisco ISE connects with the RSA SecurID authentication technology by using the RSA SecurID Agent.

Cisco ISE supports only one RSA realm.

---

**Cisco ISE and RSA SecurID Server Integration**

These are the two administrative roles involved in connecting Cisco ISE with an RSA SecurID server:

- RSA Server Administrator—Configures and maintains RSA systems and integration
- Cisco ISE Administrator—Configures Cisco ISE to connect to the RSA SecurID server and maintains the configuration
This section describes the processes that are involved in connecting Cisco ISE with the RSA SecurID server as an external identity source. For more information on RSA servers, please refer to the RSA documentation.

**RSA Configuration in Cisco ISE**

The RSA administrative system generates an sdconf.rec file, which the RSA system administrator will provide to you. This file allows you to add Cisco ISE servers as RSA SecurID agents in the realm. You have to browse and add this file to Cisco ISE. By the process of replication, the primary Cisco ISE server distributes this file to all the secondary servers.

**RSA Agent Authentication Against the RSA SecurID Server**

After the sdconf.rec file is installed on all Cisco ISE servers, the RSA agent module initializes, and authentication with RSA-generated credentials proceeds on each of the Cisco ISE servers. After the agent on each of the Cisco ISE servers in a deployment has successfully authenticated, the RSA server and the agent module together download the securid file. This file resides in the Cisco ISE file system and is in a well-known place defined by the RSA agent.

**RSA Identity Sources in a Distributed Cisco ISE Environment**

Managing RSA identity sources in a distributed Cisco ISE environment involves the following:

- Distributing the sdconf.rec and sdopts.rec files from the primary server to the secondary servers.
- Deleting the securid and sdstatus.12 files.

**RSA Server Updates in a Cisco ISE Deployment**

After you have added the sdconf.rec file in Cisco ISE, the RSA SecurID administrator might update the sdconf.rec file in case of decommissioning an RSA server or adding a new RSA secondary server. The RSA SecurID administrator will provide you with an updated file. You can then reconfigure Cisco ISE with the updated file. The replication process in Cisco ISE distributes the updated file to the secondary Cisco ISE servers in the deployment. Cisco ISE first updates the file in the file system and coordinates with the RSA agent module to phase the restart process appropriately. When the sdconf.rec file is updated, the sdstatus.12 and securid files are reset (deleted).

**Override Automatic RSA Routing**

You can have more than one RSA server in a realm. The sdopts.rec file performs the role of a load balancer. Cisco ISE servers and RSA SecurID servers operate through the agent module. The agent module that resides on Cisco ISE maintains a cost-based routing table to make the best use of the RSA servers in the realm. You can, however, choose to override this routing with a manual configuration for each Cisco ISE server for the realm using a text file called sdopts.rec through the Admin portal. Refer to the RSA documentation for information on how to create this file.

**RSA Node Secret Reset**

The securid file is a secret node key file. When RSA is initially set up, it uses a secret to validate the agents. When the RSA agent that resides in Cisco ISE successfully authenticates against the RSA server for the first time, it creates a file on the client machine called securid and uses it to ensure that the data exchanged between the machines is valid. At times, you may have to delete the securid file from a specific Cisco ISE server or a group of servers in your deployment (for example, after a key reset on the RSA server). You can use the Cisco
ISE Admin portal to delete this file from a Cisco ISE server for the realm. When the RSA agent in Cisco ISE authenticates successfully the next time, it creates a new securid file.

Note
If authentications fail after upgrading to a latest release of Cisco ISE, reset the RSA secret.

**RSA Automatic Availability Reset**

The sdstatus.12 file provides information about the availability of RSA servers in the realm. For example, it provides information on which servers are active and which are down. The agent module works with the RSA servers in the realm to maintain this availability status. This information is serially listed in the sdstatus.12 file, which is sourced in a well-known location in the Cisco ISE file system. Sometimes this file becomes old and the current status is not reflected in this file. You must remove this file so that the current status can be recreated. You can use the Admin portal to delete the file from a specific Cisco ISE server for a specific realm. Cisco ISE coordinates with the RSA agent and ensures correct restart phasing.

The availability file sdstatus.12 is deleted whenever the securid file is reset, or the sdconf.rec or sdopts.rec files are updated.

**Add RSA Identity Sources**

To create an RSA identity source, you must import the RSA configuration file (sdconf.rec). You must obtain the sdconf.rec file from your RSA administrator. To perform this task, you must be a Super Admin or System Admin.

Adding an RSA identity source involves the following tasks:

**Related Topics**

- RSA Identity Sources, on page 428
- Cisco ISE and RSA SecurID Server Integration, on page 428
- RSA Configuration in Cisco ISE, on page 429
- RSA Agent Authentication Against the RSA SecurID Server, on page 429
- RSA Identity Sources in a Distributed Cisco ISE Environment, on page 429
- RSA Server Updates in a Cisco ISE Deployment, on page 429
- Override Automatic RSA Routing, on page 429
- RSA Node Secret Reset, on page 429
- RSA Automatic Availability Reset, on page 430
- Import the RSA Configuration File, on page 430
- Configure the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files, on page 431
- Configure Authentication Control Options for RSA Identity Source, on page 432
- Configure RSA Prompts, on page 432
- Configure RSA Messages, on page 433

**Import the RSA Configuration File**

You must import the RSA configuration file to add an RSA identity source in Cisco ISE.
Configure the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files

Step 1
Log into the Cisco ISE server.

Step 2
Choose Administration > Identity Management > External Identity Sources > RSA SecurID > Add.

Step 3
Click the RSA Instance Files tab.
This page lists the sdopts.rec files for all the Cisco ISE servers in your deployment.
The Node Secret Status is displayed as Created when the user is authenticated against RSA SecurID token server. The Node Secret Status can be one of the following—Created or Not Created. The Node Secret Status is displayed as Not Created when it is cleared.

Step 4
Click the radio button next to the sdopts.rec file for a particular Cisco ISE server, and click Update Options File.
The existing file is displayed in the Current File region.

Step 5
Choose one of the following:

- Use the Automatic Load Balancing status maintained by the RSA agent—Choose this option if you want the RSA agent to automatically manage load balancing.

- Override the Automatic Load Balancing status with the sdopts.rec file selected below—Choose this option if you want to manually configure load balancing based on your specific needs. If you choose this option, you must click Browse and choose the new sdopts.rec file from the system that is running your client browser.

Step 6
Click OK.

Step 7
Click the row that corresponds to the Cisco ISE server to reset the secuirid and sdstatus.12 files for that server:
a) Click the drop-down arrow and choose Remove on Submit in the Reset secuirid File and Reset sdstatus.12 File columns.

Note The Reset sdstatus.12 File field is hidden from your view. Using the vertical and horizontal scroll bars in the innermost frame, scroll down and then to your right to view this field.
b) Click **Save** in this row to save the changes.

**Step 8**  Click **Save**.

---

**Configure Authentication Control Options for RSA Identity Source**

You can specify how Cisco ISE defines authentication failures and enable identity caching. The RSA identity source does not differentiate between “Authentication failed” and “User not found” errors and sends an Access-Reject response.

You can define how Cisco ISE should handle such failures while processing requests and reporting failures. Identity caching enables Cisco ISE to process requests that fail to authenticate against the Cisco ISE server the second time. The results and the attributes retrieved from the previous authentication are available in the cache.

**Step 1**  Choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID** > **Add**.

**Step 2**  Click the **Authentication Control** tab.

**Step 3**  Choose one of the following:

- **Treat Rejects as “authentication failed”**—Choose this option if you want the rejected requests to be treated as failed authentications.
- **Treat Rejects as “user not found”**—Choose this option if you want the rejected requests to be treated as user not found errors.

**Step 4**  Check the **Enable Passcode Caching** check box if you want Cisco ISE to store the passcode in the cache after the first successful authentication and use the cached user credentials for the subsequent authentications if they happen within the configured time period.

Enter the number of seconds for which the passcode must be stored in the cache in the **Aging Time** field. Within this period of time, the user can perform more than one authentication with the same passcode. The default value is 30 seconds. The valid range is from 1 to 300 seconds.

**Note**  Cisco ISE clears the cache after the first failed authentication. The user must enter a new, valid passcode.

**Note**  We strongly recommend that you enable this option only when you use a protocol that supports encryption of the passcode, for example, EAP-FAST-GTC.

**Step 5**  Click **Save** to save the configuration.

---

**Configure RSA Prompts**

Cisco ISE allows you to configure RSA prompts that are presented to the user while processing requests sent to the RSA SecurID server.

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.
Configure RSA Messages

Cisco ISE allows you to configure messages that are presented to the user while processing requests sent to the RSA SecurID server.

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Administration &gt; Identity Management &gt; External Identity Sources &gt; RSA SecurID.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Prompts.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the values as described in RSA SecurID Identity Source Settings.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Submit.</td>
</tr>
</tbody>
</table>

SAMLv2 Identity Provider as an External Identity Source

Security Assertion Markup Language (SAML) is an XML-based open standard data format that enables administrators to access a defined set of applications seamlessly after signing into one of those applications. SAML describes the exchange of security related information between trusted business partners. SAML enables exchange of security authentication information between an Identity Provider (IdP) and a service provider (in this case, ISE).

SAML Single Sign On (SSO) establishes a Circle of Trust (CoT) by exchanging metadata and certificates as part of the provisioning process between the IdP and the Service Provider. The Service Provider trusts the IdP’s user information to provide access to the various services or applications.

Enabling SAML SSO results in several advantages:

- It reduces password fatigue by removing the need for entering different user name and password combinations.
- It improves productivity because you spend less time re-entering credentials for the same identity.
- It transfers the authentication from your system that hosts the applications to a third party system.
- It reduces costs as fewer help desk calls are made for password reset, thereby leading to more savings.

The IdP is an authentication module that creates, maintains, and manages identity information for users, systems, or services. The IdP stores and validates the user credentials and generates a SAML response that allows the user to access the service provider protected resources.
You must be familiar with your IdP service, and ensure that it is currently installed and operational.

SAML SSO is supported for the following portals:

- Guest portal (sponsored and self-registered)
- Sponsor portal
- My Devices portal
- Certificate Provisioning portal

You cannot select IdP as external identity source for BYOD portal, but you can select an IdP for a guest portal and enable BYOD flow.

Cisco ISE is SAMLv2 compliant and supports all SAMLv2 compliant IdPs that use Base64-encoded certificates. The IdPs listed below have been tested with Cisco ISE:

- Oracle Access Manager (OAM)
- Oracle Identity Federation (OIF)
- SecureAuth
- PingOne
- PingFederate
- Azure Active Directory

The IdP cannot be added to an identity source sequence (see Identity Source Sequences, on page 438).

The SSO session will be terminated and Session Timeout error message will be displayed if there is no activity for the specified time (default is 5 minutes).

If you want to add the Sign On Again button in the Error page of the portal, add the following JavaScript in the Optional Content field in the Portal Error page:

```html
<button class="cisco-ise" data-inline="true" data-mini="true" data-theme="b" id="ui_aup_accept_button" onclick="location.href='PortalSetup.action?portal=<Portal ID>'" type="button">Sign On Again</button>
```

Add a SAML Identity Provider

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

---

**Step 1** Import the Certificate Authority (CA) certificate into the Trusted Certificate Store, if the certificate is not self-signed by the IdP. Choose **Administration > System > Certificates > Trusted Certificates > Import** to import the CA certificate.

**Step 2** Choose **Work Centers > Network Access > Ext Id Sources**.

**Step 3** Click **SAML Id Providers**.
Step 4  Click Add.
Step 5  In the SAML Identity Provider page, enter the following details:
Step 6  Click Submit.
Step 7  Go to the Portal Settings page (Guest, Sponsor, Certificate Provisioning, or My Devices portal) and select the IdP that you want to link to that portal in the Authentication Method field.

To access the Portal Settings page:


Step 8  Click Save.
Step 9  Choose Work Centers > Network Access > Ext Id Sources > SAML Id Providers. Select the IdP that is linked to that portal and click Edit.
Step 10  (Optional) In the Service Provider Info tab, add the load balancer details. You can add a load balancer in front of ISE nodes to simplify the configuration on the Identity Provider side and optimize the load on ISE nodes.

The load balancer can be a software-based or hardware-based appliance. It should be able to forward the requests to the ISE nodes in the deployment (by using the port specified at the Portal Settings page).

When a load balancer is used, only the load balancer URL is provided in the service provider metadata file. If load balancer is not configured, multiple AssertionConsumerService URLs will be included in the service provider metadata file.

Note  We recommend that you avoid using the same IP address of the load balancer at the portal FQDN setting.

Step 11  In the Service Provider Info tab, click Export to export the service provider metadata file.

The exported metadata includes the signing certificate of Cisco ISE. The signing certificate is identical to the chosen portal's certificate.

The exported metadata zip file includes a Readme file that contains the basic instructions for configuring each IdP (such as, Azure Active Directory, PingOne, PingFederate, SecureAuth, and OAM).
You must re-export the service provider metadata, if a load balancer is not configured or if there are any changes in the portal configuration, such as:

- A new ISE node is registered
- Hostname or IP address of a node is changed
- Fully qualified domain name (FQDN) of My Devices, Sponsor, or Certificate Provisioning portal is changed
- Port or interface settings are changed

If the updated metadata is not re-exported, user authentication may fail at the IdP side.

**Step 12**
Click **Browse** in the dialog box and save the compressed files locally. Unzip the metadata file folder. When you unzip the folder, you will get a metadata file with the name of the portal. The metadata file includes the Provider ID and Binding URI.

**Step 13**
Login as Admin user in IdP and import the service provider metadata file. Refer to the Identity Provider user documentation for information on how to import the service provider metadata file.

**Step 14**
In the **Groups** tab, add the required user groups.
Enter the assertion attribute that specifies the group membership of users in the **Group Membership Attribute** field.

**Step 15**
Add the user attributes in the **Attributes** tab. While adding an attribute, you can specify how the attribute appears in the assertions returned from the IdP. The name that you specify in the "Name in ISE" field will appear in the policy rules. The following data types are supported for the attributes:

- String
- Integer
- IPv4
- Boolean

Adding groups and attributes is not mandatory. These groups and attributes can be used for policy and rule settings. If you are using the sponsor portal, you can add the groups and select these groups while configuring the settings for sponsor groups.

**Step 16**
Configure the following options in the **Advanced Settings** tab:

- **Identity Attribute**—Select the attribute that specifies the identity of the user that is being authenticated. You can select the Subject Name attribute or an attribute from the Attribute drop-down list.

  **Note**
  Cisco ISE does not support SAML IdP responses that contain subject name (NameID) in transient or persistent formats. Cisco ISE cannot retrieve the Username attribute assertion from the SAML IdP response if these methods are used and the authentication will fail.

- **Email attribute**—Select the attribute that contains the email address of the sponsor. This is required to match the self-service guest requests with the sponsor.

- Select one of the following options for multi-value attributes:
  - **Each value in a separate XML element**—Click this option if your IdP returns multiple values of the same attribute in separate XML elements.
• Multiple values in a single XML element—Click this option if your IdP returns multiple values in a single XML element. You can specify the delimiter in the text box.

• Logout Settings
  • Sign Logout Requests—Check this checkbox if you want the logout requests to be signed. This option is not displayed for OAM and OIF.
  
  **Note** SecureAuth does not support SAML Logout.

  • Logout URL—This option is displayed only for OAM and OIF when a load balancer is not configured. When a user logs out of the Sponsor or My Devices portal, the user is redirected to the Logout URL at the IdP to terminate the SSO session and then redirected back to the login page.

  • Redirect Parameter Name—This option is displayed only for OAM and OIF when a load balancer is not configured. The redirect parameter is used to pass the URL of the login page to which the user must be redirected after logging out. The redirect parameter name may differ based on the IdP, for example, end_url or returnURL. This field is case sensitive.

  If logout does not work as expected, check the Identity Provider documentation for the Logout URL and Redirect Parameter Name.

**Step 17** Click **Submit**.

---

**Example**

For an example of configuring Ping Federate, see [Configure ISE 2.1 Guest Portal with PingFederate](#) SAML SSO

---

### Delete an Identity Provider

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

Ensure that the IdP that you want to delete is not linked to any portal. If the IdP is linked to any portal, the delete operation fails.

**Step 1** Choose **Work Centers > Network Access > Ext Id Sources > SAML Id Providers**.

**Step 2** Check the checkbox next to the IdP that you want to delete, and then click **Delete**.

**Step 3** Click **OK** to delete the IdP that you have selected.

---

### Authentication Failure Log

When authentication against SAML ID Store fails and the IdP redirects the user back to ISE portal (through SAML response), ISE will report a failure reason in the authentication log. For Guest portal (with or without
BYOD flow enabled), you can check the RADIUS Livelog (Operations > RADIUS > Live Log) to know the authentication failure reason. For My Devices portal and Sponsor portal, you can check the My Devices Login/Audit report and Sponsor Login/Audit report (under Operations > Reports > Guest) to know the authentication failure reason.

In case of logout failure, you can check the reports and logs to know the failure reason for My Devices, Sponsor, and Guest portal.

Authentication can fail due to the following reasons:

- SAML Response parse errors
- SAML Response validation errors (for example, Wrong Issuer)
- SAML Assertion validation errors (for example, Wrong Audience)
- SAML Response signature validation errors (for example, Wrong Signature)
- IdP signing certificate errors (for example, Certificate Revoked)

Note: Cisco ISE does not support SAML responses with encrypted assertions. If this is configured in the IdP, you will see the following error message in ISE: FailureReason=24803 Unable to find 'username' attribute in assertion.

If the authentication fails, we recommend that you check the "DetailedInfo" attribute in the authentication log. This attribute provides additional information regarding the cause of failure.

Identity Source Sequences

Identity source sequences define the order in which Cisco ISE looks for user credentials in the different databases. Cisco ISE supports the following identity sources:

- Internal Users
- Guest Users
- Active Directory
- LDAP
- RSA
- RADIUS Token Servers
- Certificate Authentication Profiles

If you have user information in more than one of the databases that are connected to Cisco ISE, you can define the order in which you want Cisco ISE to look for information in these identity sources. Once a match is found, Cisco ISE does not look any further, but evaluates the credentials, and returns the result to the user. This policy is the first match policy.
Create Identity Source Sequences

Before you begin

Ensure that you have configured your external identity sources in Cisco ISE.

To perform the following task, you must be a Super Admin or System Admin.

For allowing guest users to authenticate through Local WebAuth, you must configure both the Guest Portal authentication source and the identity source sequence to contain the same identity stores.

---

**Step 1** Choose Administration > Identity Management > Identity Source Sequences > Add.

**Step 2** Enter a name for the identity source sequence. You can also enter an optional description.

**Step 3** Check the Select Certificate Authentication Profile check box and choose a certificate authentication profile for certificate-based authentication.

**Step 4** Choose the database or databases that you want to include in the identity source sequence in the Selected List box.

**Step 5** Rearrange the databases in the Selected list in the order in which you want Cisco ISE to search the databases.

**Step 6** Choose one of the following options in the Advanced Search List area:

- **Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError** — If you want Cisco ISE to discontinue the search, if the user is not found in the first selected identity source.

- **Treat as if the user was not found and proceed to the next store in the sequence** — If you want Cisco ISE to continue searching the other selected identity sources in sequence, if the user is not found in the first selected identity source.

While processing a request, Cisco ISE searches these identity sources in sequence. Ensure that you have the identity sources in the Selected list box listed in the order in which you want Cisco ISE to search them.

**Step 7** Click Submit to create the identity source sequence that you can then use in policies.

---

Delete Identity Source Sequences

You can delete identity source sequences that you no longer use in policies.

Before you begin

- Ensure that the identity source sequence that you are about to delete is not used in any authentication policy.

- To perform the following task, you must be a Super Admin or System Admin.

---

**Step 1** Choose Administration > Identity Management > Identity Source Sequences.

**Step 2** Check the check box next to the identity source sequence or sequences that you want to delete, then click Delete.

**Step 3** Click OK to delete the identity source sequence or sequences.
Identity Source Details in Reports

Cisco ISE provides information about the identity sources through the Authentications dashlet and Identity Source reports.

Authentications Dashlet

From the Authentications dashlet, you can drill down to find more information including failure reasons. Choose Operations > RADIUS Live log to view real-time authentication summary. For more information about RADIUS Live Logs, see RADIUS Live Logs, on page 1153.

Figure 36: RADIUS Live Logs
Identity Source Reports

Cisco ISE provides various reports that include information about identity sources. See the Available Reports section for a description of these reports.
CHAPTER 16

Configure Guest Access

- Cisco ISE Guest Services, on page 443
- Guest and Sponsor Accounts, on page 444
- Guest Portals, on page 460
- Sponsor Portals, on page 474
- Monitor Guest and Sponsor Activity, on page 486
- Guest Access Web Authentication Options, on page 488

Cisco ISE Guest Services

Cisco Identity Services Engine (ISE) guest services enable you to provide secure network access to guests such as visitors, contractors, consultants, and customers. You can support guests with base Cisco ISE licenses, and you can choose from several deployment options depending on your company’s infrastructure and feature requirements.

Cisco ISE provides web-based and mobile portals to provide on-boarding for guests and employees to your company’s network and internal resources and services.

From the Admin portal, you can create and edit guest and sponsor portals, configure guest access privileges by defining their guest type, and assign sponsor privileges for creating and managing guest accounts.

- Guest Portals, on page 460
- Guest Types and User Identity Groups, on page 444
- Sponsor Portals, on page 474
- Sponsor Groups, on page 476

ISE Community Resource

For the complete list of ISE Community Resources for ISE Guest and Web Authentication, see ISE Guest Access - ISE Guest and Web Authentication.

End-User Guest and Sponsor Portals in Distributed Environment

Cisco ISE end-user web portals depend on the Administration, Policy Services, and Monitoring personas to provide configuration, session support, and reporting.
• **Administration Node**—Configuration changes that you make to users, devices, and end-user portals are written to the Administration node.

• **Policy Services Node**—The end-user portals run on a Policy Services Node, which handles all session traffic, including: network access, client provisioning, guest services, posture, and profiling. If a Policy Service Node is part of a node group, and one node fails, the other nodes detect the failure and reset any pending sessions.

• **Monitoring Node**—The Monitoring node collects, aggregates, and reports data about the end-user and device activity on the My Devices, Sponsor, and Guest portals. If the primary Monitoring node fails, the secondary Monitoring node automatically becomes the primary Monitoring node.

---

**Guest and Sponsor Accounts**

• **Guest Accounts**—Guests typically represent authorized visitors, contractors, customers, or other users who require temporary access to your network. You can also use guest accounts for employees if you prefer to use one of the guest deployment scenarios to allow employees to access the network. You can access the Sponsor portal to view guest accounts created by a sponsor and by self-registering guests.

• **Sponsor Accounts**—Use the Sponsor portal to create temporary accounts for authorized visitors to securely access your corporate network or the Internet. After creating the guest accounts, you also can use the Sponsor portal to manage these accounts and provide account details to the guests.

Guest accounts can be created by:

• **Sponsors**—On the Admin portal, you can define the access privileges and feature support for sponsors, who can access the Sponsor portal to create and manage guest accounts.

• **Guests**—Guests can also create their own accounts by registering themselves on the Self-Registered Guest portal. Based on the portal configuration, these self-registering guests may need sponsor approval before they receive their login credentials.

  Guests can also choose to access the network using the Hotspot Guest portal, which does not require the creation of guest accounts and login credentials, such as username and password.

• **Employees**—Employees who are included in identity stores (such as Active Directory, LDAP, Internal Users) can also gain access through the credentialed Guest portals (Sponsored-Guest and Self-Registered Guest portals), if configured.

After their guest accounts are created, guests can use the Sponsored-Guest portal to log in and gain access to the network.

---

**Guest Types and User Identity Groups**

Each guest account must be associated with a guest type. Guest types allow a sponsor to assign different levels of access and different network connection times to a guest account. These guest types are associated with particular network access policies. Cisco ISE includes these default guest types:

• **Contractor**—Users who need access to the network for an extended amount of time, up to a year.

• **Daily**—Guests who need access to the resources on the network for just 1 to 5 days.

• **Weekly**—Users who need access to the network for a couple of weeks.
When creating guest accounts, certain sponsor groups can be restricted to using specific guest types. Members of such a group can create guests with only the features specified for their guest type. For instance, the sponsor group, ALL ACCOUNTS, can be set up to use only the Contractor guest type, and the sponsor groups, OWN_ACCOUNTS and GROUP_ACCOUNTS, can be set up to use Daily and Weekly guest types. Also, since self-registering guests using the Self-Registered Guest portal typically need access for just a day, you can assign them the Daily guest type.

The guest type defines the user identity group for a guest.

For more information, see:
- User Identity Groups, on page 310
- Create a User Identity Group, on page 315

Create or Edit a Guest Type

Besides creating new guest types, you can edit the default Guest Types' default access privileges and settings. The changes that you make will be applied to the existing Guest accounts that were created using this Guest Type. Guest users who are logged in will not see these changes until they log out and log in again. You can also duplicate a Guest Type to create additional Guest Types with the same access privileges.

Each Guest Type has a name, description, and a list of sponsor groups that can create guest accounts with this guest type. You can designate some guest types as follows: use just for self-registering guests, or do not use to create Guest accounts (by any sponsor group).

Fill in the following fields.

- **Guest type name**—Provide a name (from 1 to 256 characters) that distinguishes this Guest Type from the other Guest Types.

- **Description**—Provide additional information (maximum of 2000 characters) about the recommended use of this Guest Type, for example, Use for self-registering Guests. Do not use for Guest account creation, and so forth.

- **Language File**—This field allows you to export and import the language file, which contains content for email subject, email message, and SMS messages in all supported languages. These languages and content are used in notifications about an expired account, and are sent to guests who are assigned to this guest type. If you are creating a new guest type, this feature is disabled until after you save the guest type. For more information about editing the language file, see Portal Language Customization, on page 548.

- **Collect Additional Data**—Click the Custom Fields... button to select which custom fields to use to collect additional data from guests using this Guest Type.

  To manage custom fields, choose Work Centers > Guest Access > Settings > Custom Fields.

- **Maximum Access Time**
  - **Account duration starts**—If you select From first login, the account start time starts when the guest user first logs in to the guest portal, and the end time equals the configured duration time. If the guest user never logs in, the account remains in the Awaiting first login state until the guest account purge policy removes the account.

  Values are from 1 to 999 days, hours, or minutes.

  A self-registered user's account starts when they create and log on to their account.
If you select **From sponsor-specified date**, enter the maximum number of days, hours, or minutes that Guests of this Guest Type can access and stay connected to the network.

If you change these settings, your changes will not apply to existing Guest accounts that were created using this Guest Type.

- **Maximum account duration**—Enter the number of days, hours, or minutes that guests assigned to this guest type can log on.

  **Note**  
  The account purge policy checks for expired guest accounts, and sends expiration notification. This policy runs every 20 minutes, so if you set the account duration to less than 20 mins, it is possible that expiration notices may not be sent out before the account is purged.

  You can specify the duration time and the days of the week when access is provided to the guests of this Guest Type by using the **Allow access only on these days and times** option.

  - The days of the week that you select limits access to the dates that are selectable in the Sponsor's calendar.

  - Maximum account duration is enforced in the sponsor portal, when the Sponsor picks duration and dates.

  The settings you make here for access time affect the time settings that are available on the sponsor portal when creating a guest account. For more information, see **Configuring the Time Settings Available to Sponsors**, on page 484.

- **Logon Options**

  - **Maximum simultaneous logins**—Enter the maximum number of user sessions that users assigned to this Guest Type can have running concurrently.

  - **When guest exceeds limit**—When you select **Maximum simultaneous logins**, you must also select the action to take when a user connects after the maximum number of log ins is reached.

    - **Disconnect the oldest connection**

    - **Disconnect the newest connection**—Optionally select **Redirect user to a portal page showing an error message**: An error message is displayed for a configurable amount of time, then the session is disconnected, and the user is redirected to the Guest portal. The error page's content is configured on the Portal Page Customization dialog, on the **Messages > Error Messages** page.

  - **Maximum devices guests can register**—Enter the maximum number of devices that can be registered to each Guest. You can set the limit to a number lower than what is already registered for the Guests of this Guest Type. This only affects newly created Guest accounts. When a new device is added, and the maximum is reached, the oldest device is disconnected.

  - **Endpoint identity group for guest device registration**—Choose an endpoint identity group to assign to guest devices. Cisco ISE provides the **GuestEndpoints** endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

  - **Allow guest to bypass the Guest portal**—Allows users to bypass the credentialed guest-type captive portal (web authentication page), and access the network by providing credentials to wired and wireless (dot1x) supplicants or VPN clients. Guest accounts change to the **Active** state, bypassing the **Awaiting Initial Login** state and the AUP page, even if the AUP is required.

  If you do not enable this setting, users must first log in through the credentialed Guest captive portal before they are able to access other parts of the network.
• **Account Expiration Notification**
  - **Send account expiration notification __ days before account expires**—Send a notification to Guests before their account expires and specify how many days, hours, or minutes before the expiration.
  - **View messages in**—Specify the language to use when displaying email or SMS notifications as you set them up.
  - **Email**—Send account expiration notices by email.
  - **Use customization from**—Apply the same customizations that you configured for the selected portal to this Guest Type's account expiration emails.
  - **Copy text from**—Reuse email text that you created for another Guest Type's account expiration email.
  - **Send test email to me at**
  - **SMS**—Send account expiration notices by SMS.

  The settings that follow for SMS are the same as for email notifications, except that you choose an SMS gateway for **Send test SMS to me**.

• **Sponsor Groups**—Specify the sponsor groups whose members can create a guest account using this guest type. Delete the sponsor groups that you do not want to have access to this guest type.

---

**What to do next**

- Create or modify sponsor groups to use this guest type. For more information, see Sponsor Groups, on page 476.
- If appropriate, assign this guest type to self-registering guests in the Self-Registered Guest portal. For more information, see Create a Self-Registered Guest Portal, on page 468.

---

**Disable a Guest Type**

You cannot delete the last remaining guest type or guest types that are being used by guest accounts. If you want to delete a guest type that is in use, first ensure that it is no longer available for use. Disabling a guest type does not affect guest accounts that were created with that guest type.

The following steps explain how to prepare for and disable a target guest type.

---

**Step 1**
Identify the sponsor groups that allow the sponsor to create guests using the target guest type. Choose Work Centers > Guest Access > Portals and Components > Sponsor Groups, and open each sponsor group and examine the This sponsor group can create accounts using these guest types list.

**Step 2**
Identify the Self-Registered portals that assign the target guest type. Choose Work Centers > Guest Access > Portals and Components > Guest Portals. Open each Self-Registered Guest portal. If the portal is using the specific guest type, expand Portal Settings, and change the assigned guest type in the field Employees using this portal as guests inherit login options from:
Step 3

Open the guest type you wish to delete, and delete all sponsor groups that you identified in the previous steps. This action effectively prevents all sponsors from using creating a new guest account with this guest type. Choose Work Centers > Guest Access > Portals and Components > Guest Type.

That's it. You can't actually delete the guest type. Make sure you don't use in any portals in the future.

Changing Guest Account Attributes

When a guest account is created, attributes are configured for that account by the Guest Type.

If you make changes to a Guest Type, active Guest accounts will take on all the attributes of the updated Guest Type, including the default access times, dates, and duration, which can then be edited. In addition, the custom fields from the original Guest Type are copied to the updated Guest Type.

A Sponsor can also extend the account duration before the time period has expired.

Configure Maximum Simultaneous Logins for Endpoint Users

You can configure the maximum number of simultaneous logins that are allowed for a guest.

When the user logs in to a guest portal, and is successfully authenticated, that user's number of existing logins is checked to see if the user has already reached the maximum number of logins. If so, the Guest user is redirected to an error page. An error page is displayed, and the session is stopped. If that user tries to access the internet again, the user's connection is redirected to the guest portal's login page.

Before you begin

Make sure that the authorization profile that you are using in the authorization policy for this portal has Access Type set to Access_Accept. If Access Type is set to Access_Reject, then maximum simultaneous logins is not enforced.

Step 1

Choose Work Centers > Guest Access > Portals & Components > Guest Type, and under Login Options:

a) Check Maximum simultaneous logins. This is already enabled on the default guest types.

b) Under When guest exceeds limit:, select Disconnect the newest connection.

c) Check Redirect user to a portal page showing an error message, and choose the maximum number of simultaneous logins to allow.

Step 2

Choose Policy > Policy Elements > Results, and create an authorization profile:

a) Under Common Tasks, check Web Redirection, then:

• In the first drop-down, choose Centralized Web Auth.

• Enter the ACL you created as part of the prerequisite.

• For Value, select the guest portal to be redirected to.

b) Scroll down in Common Tasks, and check Reauthentication, then:

• In Timer, enter the amount of time you want the error page to display before redirecting the user to the guest portal.

• In Maintain Connectivity During Reauthentication, choose Default.
Step 3 Choose Policy > Policy Sets, and create an authorization policy so that when the attribute NetworkAccess.SessionLimitExceeded is true, the user is redirected to the portal.

What to do next

You can customize the text of the error page on the Portal Page Customization tab, in the tab Messages Error Messages by changing the text of the error message key `ui_max_login_sessions_exceeded_error`.

Schedule When to Purge Expired Guest Accounts

When an active or suspended guest account reaches the end of its account duration (as defined by the sponsor when creating the account), the account expires. When guest accounts expire, the affected guests cannot access the network. Sponsors can extend expired accounts before they are purged. However, after an account is purged, sponsors must create new accounts.

When expired guest accounts are purged, the associated endpoints and reporting and logging information are retained.

Cisco ISE automatically purges expired guest accounts every 15 days, by default. The Date of next purge indicates when the next purge will occur. You can also:

- Schedule a purge to occur every X days. The first purge will occur in X days at Time of Purge, then purges occur every X days.

- Schedule a purge on a given day of the week every X weeks. The first purge occurs on the next Day of Week at Time of Purge, then purges occur every configured number of weeks on that day and time. For example, on Monday you set purges to occur on Thursday every 5 weeks. The next purge will be the Thursday of this week, not the Thursday 5 weeks from now.

- Force a purge to happen immediately by clicking Purge Now.

If the Cisco ISE server is down when the purge is scheduled to run, the purge is not executed. The purge process will run again at the next scheduled purge time, assuming the server is operational at that time.

Step 1 Choose Work Centers > Guest Access > Settings > Guest Account Purge Policy.
Step 2 Choose one of these options:

- Click Purge Now to immediately purge the expired guest account records.
- Check Schedule purge of expired guest accounts to schedule a purge.

Note After each purge is completed, the Date of next purge is reset to the next scheduled purge.

Step 3 Specify after how many days of inactivity to purge user-specific portal records maintained in the Cisco ISE database for LDAP and Active Directory users.
Step 4 Specify the number of days of inactivity to expire users in Expire portal-user information after. This setting prevents LDAP and Active Directory accounts that were never used from staying in the ISE database indefinitely.
Step 5 Click Save. If you do not want to save any updates you made to the settings, click Reset to revert to the last saved values.
Add Custom Fields for Guest Account Creation

When providing guest access, you may want to collect information from your guests beyond just their names, email addresses, and phone numbers. Cisco ISE provides custom fields that you can use to collect additional information about guests that is specific to your company’s needs. You can associate the custom fields with guest types and with the Self-Registered Guest and Sponsor portals. Cisco ISE does not provide any default custom fields.

**Step 1**
To add, edit, or delete custom fields for all Guest and Sponsor portals, choose **Guest Access > Settings > Custom Fields**.

**Step 2**
Enter the **Custom Field Name**, pick a **Data Type** from the drop-down list, and enter **Tip Text** to help provide additional information about the custom field. For instance, if you enter Date of Birth, pick Date-MDY, and enter a tip for the date format as MM/DD/YYYY.

**Step 3**
Click **Add**. The custom field appears in the list in alphabetical order or in the context of the sorted order.

**Step 4**
Click **Save**. If you do not want to save any updates you made to the settings, click **Reset** to revert to the last saved values.

**Note**
If you delete a custom field, it will no longer be available for selection in the **Custom Fields** list for guest types and in the Self-Registered Guest and Sponsor portals settings. If the field is being used, **Delete** will be disabled.

**What to do next**
You can include the desired custom fields:

- When defining a guest type so that accounts created with that guest type will include this information. See Create or Edit a Guest Type, on page 445.
- When configuring the Sponsor portal for sponsors to use when creating guest accounts. See #unique_675.
- When requesting information from self-registering guests using a Self-Registered Guest portal. See Create a Self-Registered Guest Portal, on page 468.

Specify Email Addresses and SMTP Servers for Email Notifications

Cisco ISE allows you to send emails to sponsors and guests, notifying them of information and instructions. You can configure SMTP servers to deliver these email notifications. You can also specify the email address from which the notifications will be sent to guests.

**Note**
Guest notifications require an UTF-8 compatible e-mail client.

HTML-capable e-mail client (with functionality enabled) is needed to use the single click sponsor approval feature.

**Step 1**
To specify email settings and configure SMTP servers for all Guest and Sponsor portals, choose **Work Centers > Guest Access > Settings > Guest Email Settings**.
Step 2  **Enable email notifications to guests** is checked by default. If you disable this setting, guests will not receive email notifications regardless of any other settings you may have enabled while configuring Guest and Sponsor portals.

Step 3  Enter the **Default “From” email address** that is designated for sending email notifications to guests. For example, donotreply@yourcompany.com.

Step 4  Do one of the following:
- Check **Send notifications from sponsor's email address (if sponsored)** if you want guests to receive notifications from the sponsor who created their accounts. Self-registering guests will receive notifications from the default email address.
- Check **Always send notifications from the default email address** if you want guests to receive notifications, regardless of whether they are sponsored and self-registering.

Step 5  Click **Save**. If you do not want to save any updates you made to the settings, click **Reset** to revert to the last saved values.

---

**Assign Guest Locations and SSIDs**

A Guest Location defines a name for a time zone, and is used by ISE to enforce time-related settings of logged on Guests. Guest Locations are assigned to Guest accounts by Sponsors creating a Guest account, and by self-registering Guests. The default Guest Location is San Jose. If no other Guest Locations are added, all accounts are assigned this Guest Location. You can't delete the San Jose Guest Location unless you create one or more new Locations. Unless all your Guests will be in the same time-zone as San Jose, create at least one Guest Location with the required time-zone.

**Note**

Guest access times are based on the Guest Location's time zone. A Guest user may not be able to login if the Guest Location's time zone doesn't match the system time zone. In this case, the Guest user may get an "Authentication Failed" error. You might see the "Guest active time period not yet started" error message in the debug report. As a workaround, you can adjust the Guest access start time to match the local time zone of the Guest user by using the Manage Accounts option.

The SSIDs you add here are available to Sponsor Portals, so Sponsors can tell the Guest which SSID to connect to.

You can't delete a Guest Location or a SSID if it is configured in a Sponsor portal or assigned to a Guest account.

---

**Step 1**

To add, edit or delete Guest Locations and SSIDs for Guest and Sponsor portals, choose **Work Centers > Portals & Components > Settings > Guest Locations and SSIDs**.

**Step 2**

For **Guest Locations**:

a) For each time-zone that you need to support, enter a **Location name** and pick a **Time zone** from the drop-down list.

b) Click **Add**.

**Note**

In a Guest Location, the name of the place, the name of the time zone, and the GMT offset are static; you cannot change them. The GMT offset does not change with daylight savings time changes. The GMT offsets are the opposite of what is shown in the list. For example, **Etc/GMT+3** is actually GMT-3.
Note For First-login guest type, ensure that you configure a Guest Location (time zone) only if you intend to configure the access time restrictions in the Work Centers > Guest Access > Portals & Components > Guest Types page.

Step 3 For Guest SSIDs:
   a) Enter the SSID names of the networks that will be available for guests to use at the Guest Locations.
   b) Click Add.

Step 4 Click Save. To revert to the last saved values, click Reset.

What to do next

If you added a new Guest Location or SSID, you can:
   • Provide the SSIDs for Sponsors to use when creating Guest accounts. See Portal Settings for Sponsor Portals, on page 1052.
   • Add the Guest Locations to Sponsor Groups, so Sponsors assigned to that group can use them when creating guest accounts. See Configure Sponsor Groups, on page 477.
   • Assign the Guest Locations available to self-registering guests using a Self-Registered Guest portal. See Create a Self-Registered Guest Portal, on page 468.
   • For existing guest accounts, edit them manually to add SSIDs or Locations.

Rules for Guest Password Policies

Cisco ISE has the following built-in rules for guest passwords:
   • The Guest password policy applies to sponsor portals, self registered portals, accounts uploaded in a CSV file, passwords created using the ERS API, and user created passwords.
   • Changes to the guest password policy do not affect existing accounts, until the guests passwords have expired and need to be changed.
   • Passwords are case sensitive.
   • The special characters <, >, /, and % cannot be used.
   • Minimum length and minimum required characters apply to all passwords.
   • Passwords cannot match usernames.
   • New passwords cannot match current passwords.
   • Guests do not receive notifications prior to password expiration, unlike guest account expiration. When guest passwords expire, either sponsors can reset the password to a random password or guests can log in using their current login credentials and then change their password.
Note
The guest default username is four alpabetic and password is four numeric characters. Short, easy to remember usernames and passwords are adequate for short-term guests. You can change the username and password length in ISE, if you desire.

Set the Guest Password Policy and Expiration

You can define a password policy for all Guest portals. A Guest password policy determines how the password is generated for all guest accounts. A password can be a mixture of alphabetic, numeric, or special characters. You can also set the number of days after which guest passwords will expire, requiring guests to reset their passwords.

The Guest password policy applies to sponsor portals, self registered portals, accounts uploaded in a CSV file, passwords created using the ERS API, and user created passwords.

Step 1
Choose Guest Access > Settings > Guest Password Policy.

Step 2
Enter the Minimum password length (in characters) for the guest passwords.

Step 3
Specify the characters from each character set that can be used by guests to create passwords.

Choose one of the following options under Allowed Characters and Minimums to specify the password policy for guests:

- Use all the characters from each character set.
- To prevent the use of certain characters, choose Custom from the drop-down menu, and delete these characters from the predefined and complete sets.

Step 4
Enter the minimum number of characters to use from each set.

The total number of required characters across the four character sets should not exceed the overall Minimum password length.

Step 5
Choose one of the following options under Password Expiration:

- Specify the frequency (in days) when guests have to change their passwords after they first log in. If the guests do not reset their passwords before they expire, the next time they log in to the network using their original login credentials, they are prompted to change their passwords.
- Set the passwords to never expire.

Step 6
Click Save. If you do not want to save any updates you made to the settings, click Reset to revert to the last saved values.

What to do next
You should customize the error messages that are related to the password policy to provide the password requirements.


2. Search for the keyword “policy.”
Rules for Guest Username Policies

Cisco ISE has the following built-in rules for guest username policies:

- Changes to the guest username policy do not affect existing accounts, until the guest accounts have expired and need to be changed.
- The special characters <, >, /, and % cannot be used.
- Minimum length and minimum required characters apply to all system-generated usernames, including usernames based on email addresses.
- Passwords cannot match usernames.

Set the Guest Username Policy

You can configure rules for how guest usernames are created. A generated username can be created based on the email address, or based on the first name and last name of the guest. The Sponsor can also create a random number of guest accounts to save time when creating multiple guests, or when guest names and email addresses are not available. Randomly generated guest usernames consist of a mixture of alphabetic, numeric, and special characters. These settings affect all guests.

Step 1
To define the guest username policies for all Guest and Sponsor portals, choose Work Centers > Portals & Components > Settings > Guest Username Policy.

Step 2
Enter the Minimum username length (in characters) for the guest usernames.

Step 3
Choose one of the options under Username Criteria for Known Guests to specify the policy for creating usernames for known guests.

Step 4
Choose one of the following options under Characters Allowed in Randomly-Generated Usernames to specify the policy for creating random usernames for guests:

- Use all characters from each character set.
- To prevent the use of certain characters, choose Custom from the drop-down menu, and delete these characters from the predefined and complete sets.

Step 5
Enter the minimum number of characters to use from each set.

The total number of characters from the three character sets should not exceed the number specified in Minimum username length.

Step 6
Click Save. If you do not want to save any updates you made to the settings, click Reset to revert to the last saved values.

What to do next

You should customize the error messages that are related to the username policy to provide the username requirements.


2. Search for the keyword “policy.”
**SMS Providers and Services**

SMS services are required when you and sponsors want to send SMS notifications to guests that are using credentialed Guest portals. Whenever possible, configure and provide free SMS service providers to lower your company's expenses.

Cisco ISE supports a variety of cellular service providers that provide free SMS services to their own subscribers. You can use these providers without a service contract and without configuring their account credentials in Cisco ISE. These include ATT, Orange, Sprint, TMobile, and Verizon.

You can also add other cellular service providers that offer free SMS services or a global SMS service provider, such as a Click-A-Tell. The default global SMS service provider requires a service contract and you must configure their account credentials in Cisco ISE.

- If self-registering guests pick their free SMS service provider on the Self-Registration form, SMS notifications with their login credentials are sent to them free of cost. If they do not pick their SMS service provider, then the default global SMS service provider contracted by your company is used to send the SMS notifications.

- If you plan to allow sponsors to send SMS notifications to guests whose accounts they have created, you should customize the sponsor portal and select all the appropriate SMS service providers that can be used by these sponsors. If you do not select any SMS service providers for the Sponsor portal, the default global SMS service provider contracted by your company will provide the SMS services.

SMS providers are configured as SMS Gateways in ISE. Email from ISE is converted to SMS by the SMS gateway. The SMS gateway can be behind a proxy server.

**Related Topics**

- Configure SMS Gateways to Send SMS Notifications to Guests, on page 455
- SMS Gateway Settings, on page 965

### Configure SMS Gateways to Send SMS Notifications to Guests

You must set up SMS gateways in Cisco ISE to enable:

- Sponsors to manually send SMS notifications to guests with their login credentials and password reset instructions.

- Guests to automatically receive SMS notifications with their login credentials after they successfully register themselves.

- Guests to automatically receive SMS notifications with actions to take before their guest accounts expire.

When entering information in the fields, you should update all text within [], such as [USERNAME], [PASSWORD], [PROVIDER_ID], etc., with information specific to your SMS provider's account.

**Before you begin**

Configure a default SMTP server to use for the SMS Email Gateway option.

---

**Step 1**
Choose Administration > System > Settings > SMS Gateway.

**Step 2**
Click Add.

**Step 3**
Enter an SMS Gateway Provider Name.
Step 4  Select a Provider Interface Type and enter the required information:

- **SMSEmailGateway** to send SMS via an email server.
- **SMSHTTPAPI** to send SMS via an HTTP API (GET or POST method).

For information about configuring an SMSEmailGateway and an SMSHTTPAPI gateway, see SMS Gateway Settings, on page 965.

Step 5  Check **Break up long message into multiple parts** to enable Cisco ISE to divide messages that exceed 140 bytes into multiple messages.

Most SMS providers divide long SMS messages into multiple parts automatically. MMS messages can be longer than SMS messages.

Step 6  Click **Submit**.

---

**What to do next**

If you configured a new SMS gateway, you can:

- Select the SMS service provider to use when sending SMS notifications about expiring accounts to guests. See Create or Edit a Guest Type, on page 445.

- Specify which of the configured SMS providers should display on the Self-Registration form for self-registering guests to pick from. See Create a Self-Registered Guest Portal, on page 468.

---

**Social Login for Self-Registered Guests**

Guests can select a social media provider as a way to provide credentials as a self-registered guest, instead of entering username and password in the guest portal. To enable this, you configure a social media site as an external identity source, and configure a portal that allows users to use that external identity (social media provider). Additional information about social media login for ISE can be found here: [https://communities.cisco.com/docs/DOC-73960](https://communities.cisco.com/docs/DOC-73960)

After authenticating with social media, guests can edit the information retrieved from the social media site. Even though social media credentials are used, the social media site does not know that the user has used that site's information to log in. ISE still uses the information retrieved from the Social Media site internally for future tracking.

You can configure the guest portal to prevent users from changing the information retrieved from the social media site, or even suppress display of the registration form.

**Social Login Guest Flow**

Login flow varies, depending on how you configure the Portal Settings. You can configure social media login without user registration, with user registration, or with user registration and sponsor approval.

1. **User connects to the self-registered portal, chooses to log in using social media.** If you configured an access code, the user must also enter the access code on the login page.

2. The user is redirected to the social media site for authentication. The user must approve use of their social media site's basic profile information.

3. If the login to the social media site is successful, ISE retrieves additional information about the user from the social media site. ISE uses the social media information to log the user on.
4. After login, the user may have to accept the AUP, depending on configuration.

5. The next action in the login flow depends on the configuration:
   • Without registration—Registration is done behind the scenes. Facebook provides a token for the user's device to ISE for login.
   • With registration—The user is instructed to complete a registration form that has been prepopulated with information from the social media providers. This allows the user to correct and add missing information, and submit updated information for login. If you configured a registration code in the Registration Form Settings, then they also must enter the registration code.
   • With registration and sponsor approval—In addition to allowing the user to update the social media-provided information, the user is informed that they must wait for sponsor approval. The sponsor receives an email requesting approval or denial of the account. If the sponsor approves the account, ISE emails the user that they have access. The user connects the guest portal, and is automatically logged in with social media token.

6. Registration is successful. The user is directed to the option configured in After submitting the guest form for self-registration, direct guest to on Registration Form Settings. The user's account is added to the endpoint identity group configured for the portal's guest type.

7. The user has access until the guest account expires, or the user disconnects from the network.
   If the account expired, the only way to allow the user to log in is to reactivate the account, or to delete it. The user must go through the login flow again.
   
   If a user disconnects from the network, and reconnects, the action ISE takes depends on the authorization rules. If the user hits an authorization similar to:
   
   rule if guestendpoint then permit access
   
   and the user is still in the endpoint group, then the user is redirected to the logon page. If a user still has a valid token, they are automatically logged in. If not, then they must go through registration again.
   
   If the user is no longer in the endpoint group, then they are redirected to the guest page to go through registration.

**Social Login Account Duration**

Account re-authorization varies by connection method:

• For 802.1x, the default authorization rule
  
  if guestendpoint then permit access
  
  enables a guest to reconnect if their device falls asleep, or if they roam to another building. When they reconnect, they are redirected back to guest page which either does auto login with a token, or starts registration again.

• For MAB, every time the user reconnects, they are redirected to the guest portal, and have to click the social media again. If ISE still has a token for that user's account (guest account hasn't expired), then the flow goes to log in success immediately, without having to connect with the social media provider.

To prevent every reconnect redirecting to another social login, you can configure an authorization rule that remembers the device, and permits access until the account expires. When the account expires, it is removed from the endpoint group, and the flow is redirected back to the rule for guest redirect. For example:
if wireless_mab and guest endpoint then permit access
if wireless_mab then redirect to self-registration social media portal

Reporting and User Tracking

ISE Live Logs and Facebook

- Authentication Identity Store—This is the name of the application you created in your social media app for ISE.
- Facebook username—This is the username reported by Facebook. If you allow the user to change their username during registration, the name reported by ISE is the social media username.
- SocialMediaIdentifier—This is https://facebook.com/<number>
  where number identifies the social media user.

ISE Reports—The Guest username is the user's name on the social media site.

Facebook Analytics—You can see who is using your guest network through Facebook social logon by using analytics from Facebook.

Wireless and Facebook—The User Name on the Wireless controller is the unique Facebook ID, the same as the SocialMediaIdentifier on the Live Logs. To see the setting in the Wireless UI, navigate to Monitor > Clients > Detail, and look at the User Name field.

Block a Social Media-Authenticated Guest

You can create an authorization rule to block an individual social media user. This can be useful when using Facebook for authentication, when the token has not expired. The following example shows a Wi-Fi-connected guest user blocked by using their Facebook User

For information about configuring Social Login for ISE, see Configuring Social Login, on page 458.

Configuring Social Login

Before you begin

Configure the social media site so that ISE can connect to it. Only Facebook is supported currently.

Make sure the following HTTPS 443 URLs are open through your NADs so ISE can access Facebook:

facebook.co
akamaihd.net
akamai.co
fbcdn.net
The social login URL for Facebook is HTTPS. Not all NADs support redirection to a HTTPS URL. See https://communities.cisco.com/thread/79494?start=0&tstart=0&mobileredirect=true.

Step 1
On Facebook, create a Facebook application:
   a) Log on to https://developers.facebook.com and sign up as a developer.
   b) Select Apps in the header and select Add a New App.

Step 2
Add a new Product, Facebook Login, of type Web. Click Settings, and set:
   • Client OAuth Login: NO
   • Web OAuth Login: YES
   • Force Web OAuth Reauthentication: NO
   • Embedded Browser OAuth Login: NO
   • Valid OAuth redirect URIs: add the automated redirect URLs from the ISE
   • Login from Devices: NO

Step 3
Click App Review, and select Yes on Your app is currently live and available to the public.

Step 4
In ISE, navigate to Administration > Identity Management > External Identity Sources > Social Login, and click Add to create a new social login external identity source.
   • Type—Select the type of Social Login provider. Facebook is currently the only option.
   • App ID—Enter the App ID from the Facebook application.
   • App Secret—Enter the App Secret from the Facebook application.

Step 5
In ISE, enable Social Media Login in a self-registered portal. On the portal page, navigate to Portal & Page Settings > Login Page Settings, check Allow Social Login, which causes more settings to display:
   • Show registration form after social login—This allows the user to change the information provided by Facebook.
   • Require guests to be approved—This informs the user that a sponsor must approve their account, and will send them credentials for login.

Step 6
Navigate to Administration > External Identity Sources, select the Facebook Login page, and edit your Facebook external identity source. This creates redirect URIs, which you add to the Facebook application.

Step 7
In Facebook, add the URIs from the previous step to your Facebook application.

What to do next
In Facebook, you can display data about your app, which shows the guest activity with the Facebook Social Login.
Guest Portals

When people visiting your company wish to use your company’s network to access the internet, or resources and services on your network, you can provide them network access through a Guest portal. Employees can use these Guest portals to access your company’s network, if configured.

There are three default Guest portals:

- **Hotspot Guest portal**—Network access is granted without requiring any credentials. Usually, an Acceptance of User Policy (AUP) must be accepted before network access is granted.
- **Sponsored-Guest portal**—Network access is granted by a sponsor who creates accounts for guests, and provides the Guest with login credentials.
- **Self-Registered Guest portal**—Guests can create their own accounts credentials, and may need sponsor approval before they are granted network access.

Cisco ISE can host multiple Guest portals, including a predefined set of default portals.

The default portal themes have standard Cisco branding that you can customize through the Admin portal.

Wireless setup has its own default theme (CSS) and you are able to modify some basic settings such as logo, banner, background image, coloring and fonts. In ISE, you can also choose to further customize your portal by changing more settings and go into advanced customizations.

Credentials for Guest Portals

Cisco ISE provides secured network access by requiring guests to log in using various types of credentials. You can require that guests log in using one or a combination of these credentials.

- **Username**—Required. Applies to all guests using end-user portals (except Hotspot Guest portals) and is derived from the username policy. The username policy applies only to system-generated usernames and not to usernames specified using the Guest API programming interface or the self-registering process. You can configure the policy settings that apply to usernames at **Work Centers > Guest Access > Settings > Guest Username Policy**. Guests can be notified of their username in an email, SMS, or in printed form.

- **Password**—Required. Applies to all guests using end-user portals (except Hotspot Guest portals) and is derived from the password policy. You can configure the policy settings that apply to passwords at **Work Centers > Guest Access > Settings > Guest Password Policy**. Guests can be notified of their password in an email, SMS, or in printed form.

- **Access code**—Optional. Applies to guests using the Hotspot Guest and Credentialed Guest portals. An access code is primarily a locally known code that is given to physically present guests (either visually via a whiteboard or verbally by a lobby ambassador). It would not be known and used by someone outside the premises to gain access to the network. If the Access code setting is enabled:
  - Sponsored guests are prompted to enter it on the Login page (along with a username and password).
  - Guests using the Hotspot Guest portal are prompted to enter it on the Acceptable Use Policy (AUP) page.
Guest Access with Hotspot Guest Portals

Cisco ISE provides network access functionality that includes “hotspots,” which are access points that guests can use to access the Internet without requiring credentials to log in. When guests connect to the hotspot network with a computer or any device with a web browser and attempt to connect to a website, they are automatically redirected to a Hotspot Guest portal. Both wired and wireless (Wi-Fi) connections are supported with this functionality.

The Hotspot Guest portal is an alternative Guest portal that allows you to provide network access without requiring guests to have usernames and passwords and alleviates the need to manage guest accounts. Instead, Cisco ISE works together with the network access device (NAD) and Device Registration Web Authentication (Device Registration WebAuth) to grant network access directly to the guest devices. Sometimes, guests may be required to log in with an access code. Typically, this is a code that is locally provided to guests who are physically present on a company’s premises.

If you support the Hotspot Guest portal:

- Based on the Hotspot Guest portal configuration and settings, guests are granted access to the network if the guest access conditions are met.
- Cisco ISE provides you with a default guest identity group, GuestEndpoints, which enables you to cohesively track guest devices.

Guest Access with Credentialed Guest Portals

You can use a credentialed Guest portal to identify and authorize temporary access for external users to internal networks and services, as well as to the Internet. Sponsors can create temporary usernames and passwords for authorized visitors who can access the network by entering these credentials in the portal’s Login page.

You can set up a credentialed Guest portal so that guests can log in using a username and password that is obtained:

- From a sponsor. In this guest flow, guests are greeted by a sponsor, such as a lobby ambassador, when they enter company premises and are set up with individual guest accounts.
- After they register themselves, using an optional registration code or access code. In this guest flow, guests are able to access the Internet without any human interaction and Cisco ISE ensures that these guests have unique identifiers that can be used for compliance.
- After they register themselves, using an optional registration code or access code, but only after the request for a guest account is approved by a sponsor. In this guest flow, guests are provided access to the network, but only after an additional level of screening is done.
You can also force the user to enter a new password when logging in.

Cisco ISE enables you to create multiple credentialed Guest portals, which you can use to allow guest access based on different criteria. For example, you might have a portal for monthly contractors that is separate from the portal used for daily visitors.

**Employee Access with Credentialed Guest Portals**

Employees can also access the network using Credentialed Guest Portals by signing in using their employee credentials, as long as their credentials can be accessed by the identity source sequence configured for that portal.

**Guest Device Compliance**

When guests and non-guests access the network through credentialed Guest portals, you can check their devices for compliance before they are allowed to gain access. You can route them to a Client Provisioning page and require them to first download the posture agent that checks their posture profile and verifies if their device is compliant. You can do this by enabling the option in the **Guest Device Compliance Settings** in a credentialed Guest portal, which displays the Client Provisioning page as part of the guest flow.

The Client Provisioning service provides posture assessments and remediations for guests. The Client Provisioning portal is available only with a Central Web Authorization (CWA) guest deployment. The guest login flow performs a CWA, and the credentialed Guest portal is redirected to the Client Provisioning portal after performing acceptable-use-policy and change-password checks. The posture subsystem performs a Change of Authorization (CoA) on the network access device to reauthenticate the client connection once the posture has been assessed.

**Guest Portals Configuration Tasks**

You can use a default portal and its default settings such as certificates, endpoint identity group, identity source sequence, portal themes, images, and other details provided by Cisco ISE. If you do not want to use the default settings, you should create a new portal or edit an existing one to meet your needs. You can duplicate a portal if you want to create multiple portals with the same settings.

After creating a new portal or editing a default one, you must authorize the portal for use. Once you authorize a portal for use, any subsequent configuration changes you make are effective immediately.

If you choose to delete a portal, you must first delete any authorization policy rules and authorization profiles associated with it or modify them to use another portal.

Use this table for the tasks related to configuring the different Guest portals.

<table>
<thead>
<tr>
<th>Task</th>
<th>Hotspot Guest Portal</th>
<th>Sponsored-Guest Portal</th>
<th>Self-Registered Guest Portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Policy Services, on page 463</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Add Certificates for Guest Portals, on page 463</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Create External Identity Sources, on page 464</td>
<td>Not applicable</td>
<td>Required</td>
<td>Required</td>
</tr>
</tbody>
</table>
## Enable Policy Services

To support the Cisco ISE end-user web portals, you must enable portal-policy services on the node on which you want to host them.

### Step 1
Choose Administration > System > Deployment

### Step 2
Click the node and click Edit.

### Step 3
On the General Settings tab, check Policy Service.

### Step 4
Check the Enable Session Services option.

### Step 5
Click Save.

## Add Certificates for Guest Portals

If you do not want to use the default certificates, you can add a valid certificate and assign it to a certificate group tag. The default certificate group tag used for all end-user web portals is Default Portal Certificate Group.

### Step 1
Choose Administration > System > Certificates > System Certificates.

### Step 2
Add a system certificate and assign it to a certificate group tag that you want to use for the portal.

This certificate group tag will be available to select during portal creation or editing.

### Step 3
Choose Work Centers > Guest Access > Portals & Components > Guest Portals > Create or Edit > Portal Settings.
Step 4 Select the specific certificate group tag from the Certificate group tag drop-down list that is associated with the newly added certificate.

Create External Identity Sources

Cisco ISE can connect with external identity sources such as Active Directory, LDAP, RADIUS Token, and RSA SecurID servers to obtain user information for authentication and authorization. External identity sources also include certificate authentication profiles that you need for certificate-based authentications.

Note
To work with passive identity services, which enable you to receive and share authenticated user identities, see Additional Passive Identity Service Providers, on page 368.

Step 1 Choose Administration > Identity Management > External Identity Sources.

Step 2 Choose one of these options:

• Certificate Authentication Profile for certificate-based authentications.
• Active Directory to connect to an Active Directory as an external identity source See Active Directory as an External Identity Source, on page 323 for more details.
• LDAP to add an LDAP identity source. See LDAP, on page 409 for more details.
• RADIUS Token to add a RADIUS Token server. See RADIUS Token Identity Sources, on page 423 for more details.
• RSA SecurID to add an RSA SecurID server. See RSA Identity Sources, on page 428 for more details.
• SAML Id Providers to add an identity provider (IdP), such as Oracle Access Manager. See SAMLv2 Identity Provider as an External Identity Source, on page 433 for more details.
• Social Login to add a Social Login, such as Facebook, as an external identity source, see Social Login for Self-Registered Guests, on page 456.

Configure Guest Portals to Redirect to SAML IDP Portals for Authentication

You can configure a Guest portal to allow users to be redirected to a SAML IDP portal for authentication.

Configuring the setting Allow the following identity-provider guest portal to be used for login in a guest portal (self-registered or Sponsored Guest) enables a new login area in that portal. If a user selects that login option, they are redirected to the alternate identity portal (which they don't see), and then to the SAML IDP logon portal for authentication.

For example, the Guest portal could have a link for employee login. Instead of logging in on the existing portal, the user clicks the employee logon link, and is redirected to the SAML IDP single-signon portal. The employee is either reconnected using the token from the last logon with this SAML IDP, or logs in on that SAML site. That allows the same portal to handle both guests and employees from a single SSID.

The following steps show how to configure a Guest portal that calls another portal which is configured to use a SAML IDP for authentication.

Step 1 Configure an external identity source. For more information, see SAMLv2 Identity Provider as an External Identity Source, on page 433.
Manage Users and End-User Portals

Step 2 Create a guest portal for the SAML provider. Set the Authentication method in Portal Settings to the SAML provider. The user will not see this portal, it is just a placeholder to direct the user to the SAML IDP logon page. Other portals can be configured to redirect to this sub-portal, as described next.

Step 3 Create a guest portal with the option to redirect to the guest portal for the SAML provider portal that you just created. This is the main portal, which will redirect to the sub-portal.

You may want to customize the look of this portal to make it look like the SAML provider.

a) On the Login Page Settings page of the main portal, check Allow the following identity-provider guest portal to be used for login.

b) Select the guest portal that you configured to use with the SAML provider.

Create Identity Source Sequences

Before you begin

Ensure that you have configured your external identity sources in Cisco ISE.

To perform the following task, you must be a Super Admin or System Admin.

For allowing guest users to authenticate through Local WebAuth, you must configure both the Guest Portal authentication source and the identity source sequence to contain the same identity stores.

Step 1 Choose Administration > Identity Management > Identity Source Sequences > Add.

Step 2 Enter a name for the identity source sequence. You can also enter an optional description.

Step 3 Check the Select Certificate Authentication Profile check box and choose a certificate authentication profile for certificate-based authentication.

Step 4 Choose the database or databases that you want to include in the identity source sequence in the Selected List box.

Step 5 Rearrange the databases in the Selected list in the order in which you want Cisco ISE to search the databases.

Step 6 Choose one of the following options in the Advanced Search List area:

• Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError — If you want Cisco ISE to discontinue the search, if the user is not found in the first selected identity source.

• Treat as if the user was not found and proceed to the next store in the sequence — If you want Cisco ISE to continue searching the other selected identity sources in sequence, if the user is not found in the first selected identity source.

While processing a request, Cisco ISE searches these identity sources in sequence. Ensure that you have the identity sources in the Selected list box listed in the order in which you want Cisco ISE to search them.

Step 7 Click Submit to create the identity source sequence that you can then use in policies.

Create Endpoint Identity Groups

Cisco ISE groups endpoints that it discovers in to the corresponding endpoint identity groups. Cisco ISE comes with several system-defined endpoint identity groups. You can also create additional endpoint identity groups from the Endpoint Identity Groups page. You can edit or delete the endpoint identity groups that you
have created. You can only edit the description of the system-defined endpoint identity groups; you cannot edit the name of these groups or delete them.

### Create a Hotspot Guest Portal

You can provide a Hotspot Guest portal to enable guests to connect to your network without requiring a username and password to log in. An access code can be required to log in.

You can create a new Hotspot Guest portal, or you can edit or duplicate an existing one. You can delete any Hotspot Guest portal, including the default portal provided by Cisco ISE.

Any changes that you make to the Page Settings on the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the Guest Flow diagram. If you enable a page, such as the AUP page, it appears in the flow and the guest will experience it in the portal. If you disable it, it is removed from the flow and the next enabled page displays for the guest.

All the Page Settings, except the Authentication Success Settings, are optional.

#### Before you begin

- Ensure that you have the required certificates and endpoint identity groups configured for use with this portal.

- Ensure that the WLC that guests connect to for the Hotspot portal is supported by ISE. See the [Identity Services Engine Network Component Compatibility guide](#) for your version of ISE.

### Manage Users and End-User Portals

#### Create a Hotspot Guest Portal

- **Choose** Administration > Identity Management > Groups > Endpoint Identity Groups.
- **Click Add.**
- **Enter the name for the endpoint identity group that you want to create (do not include spaces in the name of the endpoint identity group).**
- **Enter the description for the endpoint identity group that you want to create.**
- **Click the Parent Group drop-down list to choose an endpoint identity group to which you want to associate the newly created endpoint identity group.**
- **Click Submit.**

#### Create a Hotspot Guest Portal

- **Provide a unique Portal Name and a Description for the portal.** Ensure that the portal name that you use here is not used for any other end-user portals.
- **Use the Language File drop-down menu to export and import language files to use with the portal.**
- **Update the default values for ports, Ethernet interfaces, certificate group tags, endpoint identity groups, and so on in Portal Settings, and define behavior that applies to the overall portal.**
- **Update the following settings, which apply to each of the specific pages:**
  - **Acceptable Use Policy (AUP) Page Settings**—Require guests to accept an acceptable use policy.
  - **Post-Access Banner Page Settings**—Inform guests of their access status and any other additional actions, if required.
• **VLAN DHCP Release Page Settings**—Release the guest device IP address from the guest VLAN and renew it to access another VLAN on the network.
• **Authentication Success Settings**—Specify what guests should see once they are authenticated.
• **Support Information Page Settings**—Help guests provide information that the Help Desk can use to troubleshoot network access issues.

Step 7 Click Save. A system-generated URL displays as the Portal test URL, which you can use to access the portal and test it.

What to do next
You must authorize the portal in order to use it. You can also customize your portal either before or after you authorize it for use.

Create a Sponsored-Guest Portal

You can provide a Sponsored-Guest portal to enable designated sponsors to grant access to guests.

You can create a new Sponsored-Guest portal, or you can edit or duplicate an existing one. You can delete any Sponsored-Guest portal, including the default portal provided by Cisco ISE.

Any changes that you make to the Page Settings on the Portal Behavior and Flow Settings tab are reflected in the graphical flow in the Guest Flow diagram. If you enable a page, such as the AUP page, it appears in the flow and the guest will experience it in the portal. If you disable it, it is removed from the flow and the next enabled page displays for the guest.

All these page settings enable you to display an Acceptable Use Policy (AUP) for a guest and require its acceptance:

- Login Page Settings
- Acceptable Use Policy (AUP) Page Settings
- BYOD Settings

Before you begin
Ensure that you have the required certificates, external identity sources, and identity source sequences configured for use with this portal.

Step 1 Choose Work Centers > Guest Access > Portals & Components > Guest Portals > Create, Edit or Duplicate.
Step 2 If creating a new portal, in the Create Guest Portal dialog box, select Sponsored-Guest Portal as the portal type and click Continue.
Step 3 Provide a unique Portal Name and a Description for the portal.
Ensure that the portal name that you use here is not used for any other end-user portals.
Step 4 Use the Language File drop-down menu to export and import language files to use with the portal.
Step 5 Update the default values for ports, Ethernet interfaces, certificate group tags, identity source sequences, authentication method, and so on in Portal Settings, and define behavior that applies to the overall portal.
Step 6 Update the following settings, which apply to each of the specific pages:
**Create a Self-Registered Guest Portal**

You can provide a Self-Registered Guest portal to enable guests to register themselves and create their own accounts so they can access the network. You can still require that these accounts be approved by a sponsor before access is granted.

You can create a new Self-Registered Guest portal, or you can edit or duplicate an existing one. You can delete any Self-Registered Guest portal, including the default portal provided by Cisco ISE.

Any changes that you make to the Page Settings on the **Portal Behavior and Flow Settings** tab are reflected in the graphical flow in the Guest Flow diagram. If you enable a page, such as the AUP page, it appears in the flow and the guest will experience it in the portal. If you disable it, it is removed from the flow and the next enabled page displays for the guest.

---

**Step 7**

Click **Save**. A system-generated URL displays as the **Portal test URL**, which you can use to access the portal and test it.

---

**What to do next**

---

Note: The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. For example, a redirect to an external URL will not work.

You must authorize the portal in order to use it. You can also customize your portal either before or after you authorize it for use.
All these page settings enable you to display an Acceptable Use Policy (AUP) for a guest and require its acceptance:

- Login Page Settings
- Self-Registration Page Settings
- Self-Registration Success Page Settings
- Acceptable Use Policy (AUP) Page Settings
- BYOD Settings

**Before you begin**

Ensure that you have configured the required certificates, external identity sources, and identity source sequences for this portal.

---

**Step 1**

Choose **Work Centers > Guest Access > Portals & Components > Guest Portals > Create, Edit or Duplicate**.

**Step 2**

If creating a new portal, in the **Create Guest Portal** dialog box, select **Self-Registered Guest Portal** as the portal type and click **Continue**.

**Step 3**

Provide a unique **Portal Name** and a **Description** for the portal.

Ensure that the portal name that you use here is not used for any other end-user portals.

**Step 4**

Use the **Language File** drop-down menu to export and import language files to use with the portal.

**Step 5**

In **Portal Settings**, update the default values for ports, Ethernet interfaces, certificate group tags, identity source sequences, authentication method, and other settings that define behavior of this portal.

For more information about Portal Settings fields, see **Portal Settings for Credentialed Guest Portals**, on page 1039.

**Step 6**

Update the following settings, which apply to each of the specific pages:

- **Login Page Settings**—Specify guest credential and login guidelines. For more information, see **Login Page Settings for Credentialed Guest Portals**, on page 1041.
- **Self-Registration Page Settings**—Specify the information self-registering guests will read and should enter on the Self-Registration form, in addition to the guest experience after they have submitted the form.
- **Acceptable Use Policy (AUP) Page Settings**—Add a separate AUP page and define the acceptable use policy behavior for guests, including employees who use the credentialed Guest portals. For more information, see **Acceptable Use Policy (AUP) Page Settings for Credentialed Guest Portals**, on page 1045.
- **Employee Change Password Settings**—Require guests to change their password after the first time they log in.
- **Guest Device Registration Settings**—Select whether Cisco ISE automatically registers guest devices or displays a page where guests can manually register their devices.
- **BYOD Settings**—Let employees use their personal devices to access the network. For more information, see **BYOD Settings for Credentialed Guest Portals**, on page 1046. For more information, see **BYOD Settings for Credentialed Guest Portals**, on page 1046.
- **Post-Login Banner Page Settings**—Display additional information after the user successfully logs in, and before they are granted network access.
- **Guest Device Compliance Settings**—Redirects guests to the Client Provisioning page for posture assessment. For more information, see **Guest Device Compliance Settings for Credentialed Guest Portals**, on page 1048.
- **VLAN DHCP Release Page Settings**—Release the guest device IP address from the guest VLAN and renew it to access another VLAN on the network. For more information, see **BYOD Settings for Credentialed Guest Portals**, on page 1046.
• **Authentication Success Settings**—Specify where to direct guests after they are authenticated. If you redirect a Guest to an external URL after authentication, there may be a delay while the URL address is resolved and the session is redirected. For more information, see Authentication Success Settings for Guest Portals, on page 1049.

• **Support Information Page Settings**—Help guests provide information that the Help Desk can use to troubleshoot network access issues.

**Step 7** Click Save. A system-generated URL displays as the **Portal test URL**, which you can use to access the portal and test it.

---

**What to do next**

---

**Note**

The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. For example, a redirect to an external URL will not work.

You must authorize the portal in order to use it. You can also customize your portal either before or after you authorize it for use.

**Self-Registered Account Approval by Email**

When a registered guest is configured to require account approval, an email is sent to the sponsor that is configured on Self-Registration Page Settings. That email has links to deny or approve the account.

---

**Note**

If you are upgrading or restoring the database from earlier version of Cisco ISE to Cisco ISE 2.2, you must manually insert Approve/Deny links. To manually insert the Approve/Deny links

1. Select **Self-Registered Guest Portal**

2. Click on the **Portal Page Customization**

3. Click on **Insert Approve/Deny link** in the **Approval Request Email** section.

For information on configuring Approval Request emails with approval/deny links, see Configuring Account Approval Email Links, on page 471.

For example, when the sponsor opens the email, and clicks the Approve link, the action varies depending on how the approver is configured.

If **Email approval request to** is set to:

- **person being visited**
  - And the guest account **does not** require authentication - the account is approved, by a single click.
  - And the guest account **does** require authentication - the sponsor is directed to a special page on the sponsor portal, where the sponsor must enter their credentials before the account is approved.

- **sponsor email addresses listed below**—All the provided email addresses are emailed the approval links. When one of those sponsors clicks the approve or deny link, they are directed to their sponsor portal.
The sponsor provides their credentials, which are verified identified. If the sponsor group that they belong to allows them to approve the guest account, then the account is approved. If credentials fail, then the sponsor is told to log on to the sponsor portal and approve the account manually.

**Considerations**

- Only Sponsor portals using Active Directory and LDAP are supported.
- If you chose person being visited, the contents of that field, which are provided by the self-registering guest, must be the email address of a sponsor. We recommend that you customize that Self-Registered portal to change that field name to "email address of the Sponsor", or something similar. You could create a new field to capture who the guest is visiting, if necessary. When the user clicks the Register button, ISE verifies that the person being visited is a valid sponsor, and has an email address. If ISE can't find an email address for that sponsor in the identity source, then ISE displays an error message, and self-registration fails.
- When a list of sponsors is configured, the customization from the first portal is used, even if that is not the portal that the sponsor logs on to.

**Configuring Account Approval Email Links**

For more information about emailing approval links to sponsors to approve self-registering guests, see Self-Registered Account Approval by Email, on page 470.

**Step 1**
Navigate to Work Centers > Guest > Configure > Guest Portals, and select the self-registered portal that you want to configure for email account approval links.

**Step 2**
Expand the Self-Registration Page Settings tab.

**Step 3**
3. Check Require self-registered guests to be approved. This causes the Approve/Deny Link Settings section to appear at the bottom of the tab area. It also populates the email configuration of the Approval Request Email with approve and deny links.

All the possible fields that appear when you select Self-Registration Page Settings are shown below.

- **Require self-registered guests to be approved**—Specify that the self-registering guests using this portal require approval from a sponsor before receiving their guest credentials. Clicking this option displays more options for how sponsors approve a self-registered guest. For more information about this, see Self-Registered Account Approval by Email, on page 470.

- **Email approval request to**—If you select:
  - sponsor email addresses listed below, enter one or more email addresses of sponsors designated as approvers, or a mailer, to which ALL guest approval requests should be sent.
  - person being visited, then the field Require sponsor to provide credentials for authentication is displayed, and the Required option in Fields to include is enabled (if it was previously disabled). These fields are displayed on the Self-Registration form requesting this information from the self-registering guests.

- **Approve/Deny Link Settings**—This section allows you to configure:
  - Links are valid for—You can set an expiration period for the account approval links.
Authorize Portals

When you authorize a portal, you are setting up the network authorization profiles and rules for network access.

Before you begin

You must create a portal before you can authorize it.

Step 1
Set up a special authorization profile for the portal.

Step 2
Create an authorization policy rule for the profile.

Create Authorization Profiles

Each portal requires that you set up a special authorization profile for it.

Before you begin

If you do not plan to use a default portal, you must first create the portal so you can associate the portal name with the authorization profile.

Step 1

Step 2
Create an authorization profile using the name of the portal that you want to authorize for use.

What to do next

You should create a portal authorization policy rule that uses the newly created authorization profile.

Create Authorization Policy Rules for Hotspot and MDM Portals

To configure the redirection URL for a portal to use when responding to the users' (guests, sponsors, employees) access requests, define an authorization policy rule for that portal.

The url-redirect takes the following form based on the portal type, where:

\[ ip:port \] = the IP address and port number

- **Require sponsor to provide credentials for authentication**—Check this to force the sponsor to enter credentials to approve the account, even if it is not required by the configuration in this section. This field is only visible if **Require self-registered guests to be approved** is set to **person being visited**.

- **Sponsor is matched to a Sponsor Portal to verify approval privileges**—Click Details > to select the portals that are searched to verify that the sponsor is a valid system user, a member of a sponsor group, and that the members of that group have authority to approve the account. Each sponsor portal has an identity source sequence, which is used to identify the sponsor. Portals are used in the order they are listed. The first portal in the list determines the style and customization used in the sponsor portal.
PortalID = the unique portal name

For a Hotspot Guest portal:
https://ip:port/guestportal/gateway?sessionID=SessionIdValue&portal=PortalID&action=cwa&type=drw

For a Mobile Device Management (MDM) portal:
https://ip:port/mdmportal/gateway?sessionID=SessionIdValue&portal=PortalID&action=mdm

---

Step 1  Choose Policy > Policy Sets to create a new authorization policy rule under Standard policies.

Step 2  For Conditions, select an endpoint identity group that you want to use for the portal validation. For example, for the Hotspot Guest portal, select the default GuestEndpoints endpoint identity group and, for the MDM portal, select the default RegisteredDevices endpoint identity group.

**Note**  Because the Hotspot Guest portal only issues a Termination CoA, do not use Network Access:UseCase EQUALS Guest Flow as one of the validation conditions in the Guest authorization policy. Instead, match the Identity Group that the endpoint belongs to for validation. For example,

- If "GuestEndpoint" + Wireless MAB then Permit Access
- If Wireless MAB then HotSpot Redirect

Step 3  For Permissions, select the portal authorization profile that you created.

---

**Customize Guest Portals**

You can customize the portal appearance and user (guests, sponsors, or employees as applicable) experience by customizing the portal themes, changing UI elements on the portal pages, and editing error messages and notifications that display to the users. For more information about customizing portals, see Customization of End-User Web Portals , on page 519.

**Configure Periodic AUP Acceptance**

Browse to Policy > Policy Sets, and create a new authorization rule at the top of the list that redirects the Guest user to a credentialed portal when the AUP period has expired. Use conditions to compare LastAUPAcceptanceHours against the desired maximum hours, for example, LastAUPAcceptanceHours > 8. You can check for a range of hours from 8 to 999.

---

**What to do next**

To verify that the endpoint has received the AUP settings:

1. Choose Administration > Identities > EndPoints.
2. Click an endpoint to verify that the endpoint has the time that the AUP was last accepted (AUPAcceptedTime).
Forcing Periodic AUP

You can force a user to accept the AUP by using LastAUPAcceptance in a policy.

If LastAUPAcceptance >= 24: Hotspot Redirect
If LastAUPAcceptance < 24: PermitAccess
If Wireless_MAB: Hotspot Redirect

This example shows how to force AUP on a hotspot portal every 24 hours.
1. If the user accepted AUP more than 24 hours ago, then the must accept AUP (start over).
2. If the user accepted AUP less than 24 hours ago, continue the session.
3. On the first access to the network (MAB), they must accept AUP.

The same rules can be used with a credentialed portal, as long as you enable AUP for that portal.

Guest Remember Me

"Remember me" means that ISE shows a guest's username instead of MAC address in reports and logs.

When a guest first authenticates, the MAC address of their device is save in the endpoint group, and the username is used in reports. If the user disconnects, and then reconnects to the network, the MAC address is already in the endpoint group, so the user does not have to log back in again (authenticate). In this case, the username is not available, so the MAC address is used in reporting and logs.

Starting with ISE 2.3, ISE keeps the portal user ID, and uses it in some reporting, depending on the release.

- ISE 2.3 implemented this feature, but you can't turn it off.
- ISE 2.4 added the ability to turn off this feature in Guest > Settings > Logging. It is turned on by default on new installations, and disabled for upgrades and restores of previous releases.

For more information about Remember Me logging issues, see the following ISE community posting: ISE 2.3+ Remember Me guest using guest endpoint group logging display.

For more information about configuring remember me, see the ISE Guest Access Deployment guide: https://communities.cisco.com/docs/DOC-77590

For more information about which reporting methods are supported in each release, see the release notes for that release.

Sponsor Portals

The Sponsor portal is one of the primary components of Cisco ISE guest services. Using the Sponsor portal, sponsors can create and manage temporary accounts for authorized visitors to securely access the corporate network or the Internet. After creating a guest account, sponsors also can use the Sponsor portal to provide account details to the guest by printing, emailing, or texting. Before providing self-registering guests access to the company network, sponsors may be requested via email to approve their guests’ accounts.
Managing Guest Accounts on the Sponsor Portal

Sponsor Portal Log On Flow

A sponsor group specifies a set of permissions that can be assigned to a sponsor user. When a sponsor logs in to a sponsor portal:

1. ISE verifies the sponsor’s credentials.

2. If the sponsor authenticates successfully, the next step is to search all the available sponsor groups to find the ones that match that sponsor user, that is, the sponsor groups that the sponsor belongs to. A sponsor matches or belongs to a sponsor group if both:
   - The sponsor is a member of one of the configured Member Groups.
   - If you are using Other Conditions, all the conditions evaluate to true for that sponsor.

3. If the sponsor belongs to a sponsor group, then that sponsor gets the permissions from that group. A sponsor can belong to more than one sponsor group, in which case the permissions from those groups are combined. If the sponsor does not belong to any sponsor group, then the login to the sponsor portal fails.

Sponsor groups and their permissions are independent of the sponsor portals. The same algorithm for matching sponsor groups is applied regardless of which sponsor portal the sponsor logs in to.

Using a Sponsor Portal

Use a Sponsor portal to create temporary guest accounts for authorized visitors to securely access your corporate network or the Internet. After creating guest accounts, you can also use a Sponsor portal to manage these accounts and to provide account details to the guests.

On a Sponsor portal, the sponsor can create new guest accounts individually, or import a group of users from a file.

Note

An ISE administrator that was authorized from an external identity store, such as Active Directory, can be part of a Sponsor group. However, internal administrator accounts, for example, the default "admin" account, cannot be part of a Sponsor group.

There are several ways to open a Sponsor portal:

- In the Administrators console, using the Manage Accounts link. On the Administrators console, click Guest Access, then click Manage Accounts. When you click Manage Accounts, you are assigned to the default sponsor group with access to ALL_ACCOUNTS. You can create new guest accounts, but those guests cannot be notified, since there is no email address available to receive the account activation request from the guest. A Sponsor with the same privileges who logs onto the sponsor portal, and searches for those accounts, can send notification.

  This step requires that the FQDN that you configured on the sponsor portal's Portal Behavior and Flow Settings page is in your DNS server.

- In the Administrators console, on the Sponsor Portal configuration page. Click Guest Access > Portals & Components > Sponsor Portals, open a sponsor portal, and click the Portal Test URL link to the right of the Description field.
• In a browser, by opening the URL (FQDN) configured in the sponsor portal's **Portal Settings** page, which must be defined in your DNS server.

**What to do next**


**Managing Sponsor Accounts**

A sponsor user is an employee or contractor of your organization who creates and manages guest-user accounts through the sponsor portal. Cisco ISE authenticates sponsors through a local database, or through external Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory, or SAML identity stores. If you are not using an external source, you must create internal user accounts for sponsors.

**Sponsor Groups**

Sponsor groups control the permissions given to a sponsor when using any Sponsor portal. If a sponsor is a member of a sponsor group, then the sponsor receives the permissions defined in the group.

A sponsor is considered to be a member of a sponsor group if both of the following are true:

1. The sponsor belongs to at least one of the Member Groups defined in the sponsor group. A Member Group can be a User Identity Group, or a group selected from an external identity source, such as Active Directory.

2. The sponsor satisfies all of the Other Conditions specified in the sponsor group. The Other Conditions, which are optional, are conditions defined on dictionary attributes. These conditions are similar in behavior to those used in an Authorization Policy.

A sponsor can be a member of more than one sponsor group. If so, the sponsor receives the combined permissions from all of those groups, as follows:

• An individual permission such as "Delete guests' accounts" is granted if it is enabled in any of the groups.

• The sponsor can create guests using the Guest Types in any of the groups.

• The sponsor can create guests at the locations in any of the groups.

• For a numeric value such as a batch size limit, the largest value from the groups is used.

If a sponsor is not a member of any sponsor group, then the sponsor is not permitted to log in to any sponsor portal.

• ALL_ACCOUNTS—Sponsors can manage all guest accounts.

• GROUP_ACCOUNTS—Sponsors can manage the guest accounts created by sponsors from the same Sponsor Group.

• OWN_ACCOUNTS—Sponsors can manage only the Guest accounts that they created.

You can customize the features available to particular sponsor groups to limit or expand the functionality of the Sponsor portal. For example:

**Related Topics**

Create Sponsor Accounts and Assign to Sponsor Groups

To create internal sponsor user accounts and specify the sponsors who can use the Sponsor portals:

Step 1
Choose Administration > Identity Management > Identities > Users. Assign the internal sponsor user account to the appropriate user identity group.

Note
The default Sponsor Groups have the default Identity Group Guest_Portal_Sequence assigned to them.

Step 2
Choose Work Centers > Guest Access > Portals & Components > Sponsor Groups > Create, Edit or Duplicate and click Members. Map the sponsor user identity groups to sponsor groups.

What to do next
You can also create additional user identity groups specific to your organization to use with sponsors. Choose Administration > Identity Management > Groups > User Identity Groups.

Configure Sponsor Groups

Cisco provides default sponsor groups. If you do not want to use the default options, you can either create new sponsor groups or edit the default sponsor groups and change the settings. You can also duplicate a sponsor group to create more sponsor groups with the same settings and privileges.

You can disable a sponsor group, which prevents the members of the sponsor group from logging into the Sponsor portal. You can delete any of the sponsor groups, except the default sponsor groups provided by Cisco ISE.

Step 1
Choose Work Centers > Guest Access > Portals and Components > Sponsor Groups > Create, Edit or Duplicate

Step 2
Enter the Sponsor group name and Description.

Step 3
Match Criteria—The settings in this section determine if a sponsor is a member of this group.

- **Member Groups**—Click Members to select one or more user (identity) groups and groups from external identity sources, and add those groups. In order for a user to be a member of this sponsor group, they must belong to at least one of the configured groups.

- **Other conditions**—Click Create New Condition to build one or more conditions that a sponsor must match to be included in this sponsor group. You can use authentication attributes from Active Directory, LDAP, SAML, and ODBC identity stores, but not RADIUS Token or RSA SecurID stores. You can also use internal user attributes. Conditions have an attribute, and operator, and a value.

  - To create a condition using the internal dictionary attribute Name, prefix the identity group name with User Identity Groups. For example:

    \[
    \text{InternalUser:Name \text{EQUALS} bsmit}
    \]

    This means that only internal users with the Name "bsmith" can belong to this sponsor group.

  - To create a condition using the ExternalGroups attribute of an Active Directory instance, select the AD “Primary Group” for the sponsor users you want to match. For example, \text{AD1:LastName \text{EQUALS} Smith} is true if the user’s name is Smith.
In addition to matching one or more of the configured member groups, a sponsor must also match all the conditions you create here. If an authenticating sponsor user meets the matching criteria for multiple sponsor groups, then that user is granted permissions as follows:

- An individual permission, such as Delete guests' accounts is granted if it is enabled in any of the matching groups.
- The sponsor can create guests using the Guest Types in any of the matching groups.
- The sponsor can create guests using the Guest Types in any of the matching groups.
- The sponsor can create guests at the locations in any of the matching groups.
- For a numeric value such as a batch size limit, the largest value from the matching groups is used.

You can create Matching Criteria that contain Member Groups only, or Other Conditions only. If you only specify Other Conditions, then membership of a sponsor in the sponsor group is determined solely by matching dictionary attributes.

**Step 4**

To specify which guest types that sponsors based on this sponsor group can create, click inside the box under **This sponsor group can create accounts using these guest types**, and select one or more guest types.

You can create more guest types to assign to this sponsor group by clicking the link under **Create Guest Types at**. After you create a new guest type, save, close, and reopen the sponsor group before you can select that new guest type.

**Step 5**

Use **Select the locations that guests will be visiting** to specify the locations (used to set the guest time zones) that sponsors in this sponsor group can choose from when creating guest accounts.

You can add more locations to choose from by clicking the link under **Configure guest locations at** and adding guest locations. After you create a new guest location, save, close, and reopen the sponsor group before you can select that new guest location.

This does not restrict guests from logging in from other locations.

**Step 6**

Under **Automatic guest notification**, check **Automatically email guests upon account creation if email address is available** if you want to save your sponsors the step of clicking **Notify** after creating a user. This causes a window to popup saying that an email was sent. Checking this also adds a header to the sponsor portal that says **Guest notifications are sent automatically**.

**Step 7**

Under **Sponsor Can Create**, configure options that sponsors in this group have for creating guest accounts.

- **Multiple guest accounts assigned to specific guests (Import)**—Enable the sponsor to create multiple guest accounts by importing guest details such as first name and last name from a file.
  
  If this option is enabled, the **Import** button displays on the **Create Accounts** page of the Sponsor portal. The Import option is only available on desktop browsers (not mobile), such as Internet Explorer, Firefox, Safari, and so forth

- **Limit to batch of**—If this sponsor group is allowed to create multiple accounts simultaneously, specify the number of guest accounts that can be created in a single import operation.

  Although a sponsor can create a maximum of 10,000 accounts, we recommend that you limit the number of accounts you create, due to potential performance issues.

- **Multiple guest accounts to be assigned to any guests (Random)**—Enable the sponsor to create multiple random guest accounts as placeholders for guests who are not known as yet, or to create many accounts quickly.

  If this option is enabled, the **Random** button displays on the **Create Accounts** page of the Sponsor portal.
• **Default username prefix**—Specify a username prefix that sponsors can use when creating multiple random guest accounts. If specified, this prefix appears in the Sponsor Portal when creating random guest accounts. In addition, if **Allow sponsor to specify a username prefix** is:
  • **Enabled**—The sponsor can edit the default prefix in the Sponsor portal.
  • **Not enabled**—The sponsor cannot edit the default prefix in the Sponsor portal.

If you do not specify a username prefix or allow the sponsor to specify one, then the sponsor will not be able to assign username prefixes in the Sponsor portal.

• **Allow sponsor to specify a username prefix**—If this sponsor group is allowed to create multiple accounts simultaneously, specify the number of guest accounts that can be created in a single import operation.

Although a sponsor can create a maximum of 10,000 accounts, we recommend that you limit the number of accounts you create, due to potential performance issues.

**Step 8**

Under **Sponsor Can Manage**, you can restrict which guests accounts the members of this sponsor group can view and manage.

  • **Only accounts sponsor has created**—Sponsors in this group can view and manage only the guest accounts that they have created, which is based on the Sponsor’s email account.

  • **Accounts created by members of this sponsor group**—Sponsors in this group can view and manage the guest accounts created by any sponsor in this sponsor group.

  • **All guest accounts**—Sponsors view and manage all pending guest accounts.

**Step 9**

Under **Sponsor Can**, you can provide more privileges related to guest passwords and accounts to the members of this sponsor group.

  • **Update guests’ contact information (email, Phone Number)**—For guest accounts that they can manage, allow the sponsor to change a guest's contact information

  • **View/print guests’ passwords**—When this is checked the sponsor can print passwords for guests. The sponsor can see the passwords for guests on the Manage Accounts page and in the details for a guest. When this is not checked, the sponsor can't print the password, but the user can still get the password through email or SMS, if configured.

  • **Send SMS notifications with guests’ credentials**—For guest accounts that they can manage, allow the sponsor to send SMS (text) notifications to guests with their account details and login credentials.

  • **Reset guest account passwords**—For guest accounts that they can manage, allow the sponsor to reset passwords for guests to a random password generated by Cisco ISE.

  • **Extend guests’ accounts**—For guest accounts that they can manage, allow the sponsor to extend them beyond their expiration date. The sponsor is automatically copied on email notifications sent to guests regarding their account expiration.

  • **Delete guests’ accounts**—For guest accounts that they can manage, allow the sponsor to delete the accounts, and prevent guests from accessing your company's network.

  • **Suspend guests’ accounts**—For guest accounts that they can manage, allow the sponsor to suspend their accounts to prevent guests from logging in temporarily.

This action also issues a Change of Authorization (CoA) Terminate to remove the suspended guests from the network.
Configure Account Content for Sponsor Account Creation

You can configure the type of user data that your guests and sponsors must provide to create a new guest account. Some fields are required to identify an ISE account, but you can eliminate other fields, and add your own custom fields.

To configure fields for account creation by Sponsors:

1. In ISE, choose Work Centers > Guest Access > Portals & Components > Sponsor Portals, and edit your sponsor portal.
2. Select the Portal Page Customization tab.
3. Scroll down and select Create Account for Known Guests.
4. On the Preview display on the right, select Settings.

These settings determine which fields display and are required for guest accounts when they are created on the sponsor portal. This configuration applies to Known, Random, and Imported guest types. The template that the sponsor downloads to import new users is created dynamically, so that only the fields set in Known Guests are included.

Import Username and Password for Accounts

Sponsors can import username and password, but those rows are not added to the CSV template when the sponsor downloads it. The sponsor can add those headings. They must be named properly in order for the ISE to recognize the columns:

- Username—Can be either User Name or UserName.
- Password—Must be password.
Configure a Sponsor Portal Flow

You can use a default portal and its default settings such as certificates, endpoint identity group, identity source sequence, portal themes, images, and other details provided by Cisco ISE. If you do not want to use the default settings, you should create a new portal or edit an existing one to meet your needs. You can duplicate a portal if you want to create multiple portals with the same settings.

You may want to create multiple sponsor portals if your company has different branding for your corporate office and its retail locations, or if your company has different product brands, or if a city's offices want different themed portals for the fire, police, and other departments.

These are the tasks related to configuring a Sponsor portal.

**Before you begin**

Configure or edit existing sponsor groups for your site, as described in Configure Sponsor Groups, on page 477.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Enable Policy Services, on page 481.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Add Certificates for Guest Services, on page 481.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Create External Identity Sources, on page 482.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Create Identity Source Sequences, on page 482.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Create a Sponsor Portal, on page 483.</td>
</tr>
<tr>
<td>Step 6</td>
<td>(Optional) Customize Sponsor Portals, on page 484.</td>
</tr>
</tbody>
</table>

**Enable Policy Services**

To support the Cisco ISE end-user web portals, you must enable portal-policy services on the node on which you want to host them.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; System &gt; Deployment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click the node and click Edit.</td>
</tr>
<tr>
<td>Step 3</td>
<td>On the General Settings tab, check Policy Service.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Check the Enable Session Services option.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

**Add Certificates for Guest Services**

If you do not want to use the default certificates, you can add a valid certificate and assign it to a certificate group tag. The default certificate group tag used for all end-user web portals is Default Portal Certificate Group.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Chose Administration &gt; System &gt; Certificates &gt; System Certificates.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Add a system certificate and assign it to a certificate group tag that you want to use for the portal.</td>
</tr>
</tbody>
</table>
Create External Identity Sources

Cisco ISE can connect with external identity sources such as Active Directory, LDAP, RADIUS Token, and RSA SecurID servers to obtain user information for authentication and authorization. External identity sources also include certificate authentication profiles that you need for certificate-based authentications.

To work with passive identity services, which enable you to receive and share authenticated user identities, see Additional Passive Identity Service Providers, on page 368.

Create Identity Source Sequences

Before you begin

Ensure that you have configured your external identity sources in Cisco ISE.

To perform the following task, you must be a Super Admin or System Admin.

For allowing guest users to authenticate through Local WebAuth, you must configure both the Guest Portal authentication source and the identity source sequence to contain the same identity stores.

Create External Identity Sources

This certificate group tag will be available to select during portal creation or editing.

Step 3
Choose Work Centers > Guest Access > Portals & Components > Sponsor Portals > Create or Edit > Portal Settings.

Step 4
Select the specific certificate group tag from the Certificate Group Tag drop-down list that is associated with the newly added certificate.

Step 1
Choose Administration > Identity Management > External Identity Sources.

Step 2
Choose one of these options:
- **Certificate Authentication Profile** for certificate-based authentications.
- **Active Directory** to connect to an Active Directory as an external identity source See Active Directory as an External Identity Source, on page 323 for more details.
- **LDAP** to add an LDAP identity source. See LDAP, on page 409 for more details.
- **RADIUS Token** to add a RADIUS Token server. See RADIUS Token Identity Sources, on page 423 for more details.
- **RSA SecurID** to add an RSA SecurID server. See RSA Identity Sources, on page 428 for more details.
- **SAML Id Providers** to add an identity provider (IdP), such as Oracle Access Manager. See SAMLv2 Identity Provider as an External Identity Source, on page 433 for more details.
- **Social Login** to add a Social Login, such as Facebook, as an external identity source, see Social Login for Self-Registered Guests, on page 456.

Step 1
Choose Administration > Identity Management > Identity Source Sequences > Add.

Step 2
Enter a name for the identity source sequence. You can also enter an optional description.
Step 3  Check the Select Certificate Authentication Profile checkbox and choose a certificate authentication profile for certificate-based authentication.

Step 4  Choose the database or databases that you want to include in the identity source sequence in the Selected List box.

Step 5  Rearrange the databases in the Selected list in the order in which you want Cisco ISE to search the databases.

Step 6  Choose one of the following options in the Advanced Search List area:

- Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError — If you want Cisco ISE to discontinue the search, if the user is not found in the first selected identity source.

- Treat as if the user was not found and proceed to the next store in the sequence — If you want Cisco ISE to continue searching the other selected identity sources in sequence, if the user is not found in the first selected identity source.

While processing a request, Cisco ISE searches these identity sources in sequence. Ensure that you have the identity sources in the Selected list box listed in the order in which you want Cisco ISE to search them.

Step 7  Click Submit to create the identity source sequence that you can then use in policies.

Create a Sponsor Portal

You can provide a Sponsor portal to enable sponsors to create, manage, and approve accounts for guests who want to connect to your network to access the internet and internal resources and services.

Cisco ISE provides you with a default Sponsor portal that you can use without having to create another one. However, you can create a new Sponsor portal, or you can edit or duplicate an existing one. You can delete any of these portals, except the default Sponsor portal.

Any changes that you make to the Page Settings on the Portal Behavior and Flow Settings tab are reflected in the graphical flow in the Sponsor Flow diagram. If you enable a page, such as the AUP page, it appears in the flow and the sponsor will experience it in the portal. If you disable it, it is removed from the flow and the next enabled page displays for the sponsor.

Before you begin

Ensure that you have the required certificates, external identity sources, and identity source sequences configured for use with this portal.

Step 1  Configure the Portal Settings page, as described in Portal Settings for Sponsor Portals, on page 1052.

Step 2  Configure the Login Settings page, as described in Login Settings for Sponsor Portals, on page 1054.

Step 3  Configure the Acceptable Use Policy (AUP) Page Settings page, as described in Acceptable Use Policy (AUP) Settings for Sponsor Portals, on page 1055.

Step 4  Configure the Sponsor Change Password Settings page, as described in Set the Guest Password Policy and Expiration, on page 453 and in Rules for Guest Password Policies, on page 452.

Step 5  Configure the Post-Login Banner Page Settings page, as described in Post-Login Banner Settings for Sponsor Portals, on page 1055.

Step 6  Sponsor Portal Application Settings refers you to the Portal Customization tab if you with to customize the portal.
Step 7 Click Save.

Customize Sponsor Portals

You can customize the portal appearance and user experience by customizing the portal themes, changing UI elements on the portal pages, and editing error messages and notifications that display to the users. For more information about customizing portals, see Customization of End-User Web Portals, on page 519.

Configuring Account Content for Sponsor Account Creation

You can configure the type of user data that your guests and sponsors must provide to create a new guest account. Some fields are required to identify an ISE account, but you can eliminate other fields, and add your own custom fields.

To configure fields for account creation by Sponsors:

1. In ISE, choose Work Centers > Guest Access > Portals & Components > Sponsor Portals, and edit your sponsor portal.

2. Select the Portal Page Customization tab.

3. Scroll down and select Create Account for Known Guests.

   • On the Preview display on the right, select Settings.

These settings determine which fields display and are required for guest accounts when they are created on the sponsor portal.

This configuration applies to Known, Random, and Imported guest types. The template that the sponsor downloads to import new users is created dynamically, so that only the fields set in Known Guests are included.

Sponsor Import Usernames and Passwords for Accounts

Sponsors can import username and password, but those rows are not added to the template when the sponsor downloads it. The sponsor can add those headings. They must be named properly in order for the ISE to recognize the columns:

• Username—Can be either User Name or UserName

• Password—Must be password

Configuring the Time Settings Available to Sponsors

When sponsors create a new guest account, they configure the time that the account is active. You configure the options that are available to the sponsor, to allow them to set the account duration, and the start and end times. These options are configured by guest type. The sponsor sees the results under the heading Access Information.

The Guest Type settings that control sponsor portal account time options are under the heading Maximum Access Time, and are described below:

• From first login - The sponsor portal shows Duration, and From First Login displays under the field:
The guest type setting Maximum account duration determines which values the Sponsor can enter for duration.

- From sponsor-specified date (or date of self-registration, if applicable) - The sponsor can choose between setting the duration as End of business day, or, by unchecking that field, the duration, start and end times.

The guest type settings to control the duration time and effective dates are under the heading Allow access only on these days and times.

- The days of the week that you select limits the dates that are selectable in the Sponsor's calendar.
- Maximum account duration is enforced in the sponsor portal when picking duration and dates.

**Sponsors Cannot Log In to the Sponsor Portal**

**Problem**

The following error message appears when a sponsor tries to log in to the Sponsor portal:

“Invalid username or password. Please try again.”
Causes

• The sponsor has entered invalid credentials.

• The sponsor is not valid because the user record is not present in the database (Internal Users or Active Directory).

• The sponsor group to which the sponsor belongs is disabled.

• The Sponsor's user account is not a member of an active/enabled Sponsor Group, which means the Sponsor user's Identity Group is not a member of any Sponsor Group.

• The sponsor’s internal user account is disabled (suspended).

Solution

• Verify the user’s credentials.

• Enable the sponsor group.

• Reinstate the user account if disabled.

• Add the sponsor user's Identity Group as a member of a Sponsor Group.

Monitor Guest and Sponsor Activity

Cisco ISE provides various reports and logs that allow you to view endpoint and user management information and guest and sponsor activity. Some of the Cisco ISE 1.2 reports have been deprecated, but the information can be viewed in other reports.

You can run these reports either on demand or on a scheduled basis.

---

Step 1  Choose Operations > Reports.
Step 2  Under the Report Selector, expand the Guest Access Reports and Endpoints and Users selections to view the various guest, sponsor, and endpoint related reports.
Step 3  Select the report and choose the data with which you want to search using the Filters drop-down list.
        You can use filters on username, portal name, device name, endpoint identity group and other such data.
Step 4  Select the Time Range during which you want to view the data.
Step 5  Click Run.

Metrics Dashboard

Cisco ISE provides an at-a-glance view of Authenticated Guests and Active Endpoints in the network in a metrics dashboard that appears on the Cisco ISE Home page.
For Hotspot flow, the endpoints are not displayed on the Authenticated Guests dashlet.

AUP Acceptance Status Report

The AUP Acceptance Status report displays the acceptance status of the Acceptable Use Policy (AUP) by guests from all the Guest portals. This report is available at: Operations > Reports > Guest Access Reports > AUP Acceptance Status.

You can use the report to track all the accepted and denied AUP connections for a given period of time.

Guest Accounting Report

The Guest Accounting report displays the guest login history for an indicated time period. This report is available at: Operations > Reports > Guest Access Reports > Guest Accounting.

Master Guest Report

The Master Guest report combines data from various reports into a single view enabling you to export data from different reporting sources. You can add more data columns and remove the ones you do not want to view or export. This report is available at Operations > Reports > Guest Access Reports > Master Guest.

It now includes information that used to be in the deprecated Guest Activity Report.

This report collects all guest activity and provides details about the websites that guest users visit. You can use this report for security auditing purposes to see when guest users accessed the network and what they did on it. To view the guests’ Internet activity, such as the URLs of the websites that they visited, you must first:

- Enable the passed authentications logging category. Choose Administration > System > Logging > Logging Categories and select Passed authentications.
- Enable these options on the firewall used for guest traffic:
  - Inspect HTTP traffic and send data to Cisco ISE Monitoring node. Cisco ISE requires only the IP address and accessed URL for the Guest Activity report; so, limit the data to include just this information, if possible.
  - Send syslogs to Cisco ISE Monitoring node.

Sponsor Login and Audit Report

The Sponsor Login and Audit report is a combined report that tracks:

- Login activity by the sponsors at the Sponsor portal.
- Guest-related operations performed by the sponsors in the Sponsor portal.

This report is available at Operations > Reports > Guest Access Reports > Sponsor Login and Audit.
Audit Logging for Guest and Sponsor Portals

During specific actions within the Guest and Sponsor portals, audit log messages are sent to the underlying audit system. By default, these messages appear in the /opt/CSCOcpm/logs/localStore/iseLocalStore.log file. You can configure these messages to be sent by syslog to the monitoring and troubleshooting system and log collector. The monitoring subsystem presents this information in the appropriate sponsor and device audit logs and guest activity logs.

Guest login flow is logged in the audit logs regardless of whether the guest login has passed or failed.

Guest Access Web Authentication Options

Cisco ISE supports several deployment options to enable secure guest access through Cisco ISE Guest and Web Authentication Services. You can provide wired or wireless guest connectivity using Local or Central Web Authentication and Device Registration Web Authentication.

- Central Web Authentication (CentralWebAuth)—Applies to all Guest portals. Web authentication is done by a central Cisco ISE RADIUS server for both wired and wireless connection requests. Authentication of the guest device is done after an optional access code is entered by the guest at the Hotspot Guest portals and a username and password are entered by the guest at the Credentialed Guest portals.

  **Note** When using redirection to a browser for user credentials (CWA), users whose browsers open multiple tabs at startup are not supported. During redirection, if the browser opens more than one tab, ISE redirects to every tab, the user can login to the portal but ISE will not correctly authorize the session and the user fails to gain access.

  To work around this problem, the user must close all but one tab on their browser.

- Local Web Authentication (LocalWebAuth)—Applies to the Credentialed Guest portals. Serving of the web pages to the guest is done locally either on a network access device (NAD) such as a switch for a wired connection or by the wireless LAN controller (WLC) for a wireless connection. Authentication of the guest device is done after a username and password are entered by the guest at the Credentialed Guest portals.

- Device Registration Web Authentication (DeviceRegistrationWebAuth)—Applies only to the Hotspot Guest portal. Web authentication is done after the guest device is registered and authorized for use by Cisco ISE. Guests are directed to the Hotspot Guest portal where they can gain access to the network through either a wired or wireless connection (without entering a username or password).

ISE Community Resource

For information on how to configure Cisco ISE with Cisco Wireless Controller to provide guest access, see [How-To_93_ISE_20_Wireless_Guest_Setup_Guide](http://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/115732-central-web-auth-00.html).

NAD with Central WebAuth Process

In this scenario, the network access device (NAD) makes a new authorization request to the Cisco ISE RADIUS server from an unknown endpoint connection. The endpoint then receives a url-redirect to Cisco ISE.

Note

The webauth-vrf-aware command is supported only in IOS XE 3.7E, IOS 15.2(4)E or later versions. Other switches do not support WebAuth URL redirect in virtual routing and forwarding (VRF) environment. In such cases, as a workaround, you can add a route in the global routing table to leak the traffic back into the VRF.

If the guest device is connected to a NAD, the guest service interaction takes the form of a MAC Authentication Bypass (MAB) request that leads to a Guest portal Central WebAuth login. The following is an outline of the subsequent Central Web Authentication (Central WebAuth) process, which applies to both wireless and wired network access devices.

1. The guest device connects to the NAD through a hard-wired connection. There is no 802.1X supplicant on the guest device.

2. An authentication policy with a service type for MAB allows a MAB failure to continue and return a restricted network profile containing a url-redirect for the Central WebAuth user interface.

3. The NAD is configured to authenticate MAB requests to the Cisco ISE RADIUS server.

4. The Cisco ISE RADIUS server processes the MAB request and does not find an endpoint for the guest device.

This MAB failure resolves to the restricted network profile and returns the url-redirect value in the profile to the NAD in an access-accept. To support this function, ensure that an authorization policy exists and features the appropriate wired or wireless MAB (under compound conditions) and, optionally, "Session:Posture Status=Unknown” conditions. The NAD uses this value to redirect all guest HTTPS traffic on the default port 8443 to the url-redirect value.

The standard URL value in this case is:


5. The guest device initiates an HTTP request to redirect URL via a web browser.

6. The NAD redirects the request to the url-redirect value returned from the initial access-accept.

7. The gateway URL value with action CWA redirects to the Guest portal login page.

8. The guest enters their login credentials and submits the login form.

9. The guest server authenticates the login credentials.

10. Depending on the type of flow, the following occurs:

    • If it is a non-posture flow (authentication without further validation), where the Guest portal is not configured to perform client provisioning, the guest server sends a CoA to the NAD. This CoA causes the NAD to reauthenticate the guest device using the Cisco ISE RADIUS server. A new access-accept is returned to the NAD with the configured network access. If client provisioning is not configured and the VLAN needs to be changed, the Guest portal performs VLAN IP renew. The guest does not have to re-enter login credentials. The username and password entered for the initial login are used automatically.
If it is a posture flow, where the Guest portal is configured to perform client provisioning, the guest device web browser displays the Client Provisioning page for posture agent installation and compliance. (You can also optionally configure the client provisioning resource policy to feature a “NetworkAccess:UseCase=GuestFlow” condition.)

Because there is no client provisioning or posture agent for Linux, the Guest portal redirects to the Client Provisioning portal, which in turn redirects back to a guest authentication servlet to perform optional IP release/renew and then CoA.

With redirection to the Client Provisioning portal, the Client Provisioning service downloads a non-persistent web agent to the guest device and performs a posture check of the device. (You can optionally configure the posture policy with a “NetworkAccess:UseCase=GuestFlow” condition.)

If the guest device is non-compliant, ensure that you have configured an authorization policy that features “NetworkAccess:UseCase=GuestFlow” and “Session:Posture Status=NonCompliant” conditions.

When the guest device is compliant, ensure that you have an authorization policy configured with the conditions “NetworkAccess:UseCase=GuestFlow” and “Session:Posture Status=Compliant.” From here, the Client Provisioning service issues a CoA to the NAD. This CoA causes the NAD to reauthenticate the guest using the Cisco ISE RADIUS server. A new access-accept is returned to the NAD with the configured network access.

“NetworkAccess:UseCase=GuestFlow” can also apply for Active Directory (AD) and LDAP users who log in as guests.

Wireless LAN Controller with Local WebAuth Process

In this scenario, the guest logs in and is directed to the wireless LAN controller (WLC). The WLC then redirects the guest to a Guest portal, where they are prompted to enter their login credentials, accept an optional Acceptable Use Policy (AUP), and perform an optional password change. When this is complete, the guest device’s browser is redirected back to the WLC to provide login credentials via a POST.

The WLC can now log the guest in via the Cisco ISE RADIUS server. When this is complete, the WLC redirects the guest device's browser to the original URL destination. The Wireless LAN Controller (WLC) and the network access devices (NAD) requirements to support the original URL redirect for guest portals are WLC 5760 and Cisco Catalyst 3850, 3650, 2000, 3000, and 4000 Series Access Switches running releases IOS-XE 3.6.0.E and 15.2(2)E.
Wired NAD with Local WebAuth Process

In this scenario, the Guest portal redirects the guest login request to the switch (wired NAD). The login request is in the form of an HTTPS URL posted to the switch and contains the login credentials. The switch receives the guest login request and authenticates the guest using the configured Cisco ISE RADIUS server.

1. Cisco ISE requires a login.html file with the HTML redirect to be uploaded to the NAD. This login.html file is returned to the browser of the guest device for any HTTPS request made.

2. The browser of the guest device is redirected to the Guest portal where the guest’s login credentials are entered.

3. After the Acceptable Use Policy (AUP) and change password are processed, both of which are optional, the Guest portal redirects the browser of the guest device to post the login credentials on the NAD.

4. The NAD makes a RADIUS request to the Cisco ISE RADIUS server to authenticate and authorize the guest.

IP Address and Port Values Required for the Login.html Page

The IP address and port values must be changed in the following HTML code for the login.html page to those values being used by the Cisco ISE Policy Services nodes. The default port is 8443, but you can change this value, so ensure that the value you assign to the switch matches the setting in Cisco ISE.

```html
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html>
```
Because the custom login page is a public web form, consider these guidelines:

- The login form must accept user entries for the username and password and must show them as `uname` and `pwd`.
- The custom login page should follow best practices for a web form, such as page timeout, hidden password, and prevention of redundant submissions.

**HTTPS Server Enabled on the NAD**

To use web-based authentication, you must enable the HTTPS server within the switch using the `ip http secure-server` command.

**Support for Customized Authentication Proxy Web Pages on the NAD**

You can upload custom pages for success, expiry, and failure to the NAD. Cisco ISE does not require any specific customization, so you can create these pages using the standard configuration instructions included with the NAD.

**Configure Web Authentication on the NAD**

You need to complete the web authentication on the NAD by replacing the default HTML pages with your custom files.

**Before you begin**

During web-based authentication, create four substitute HTML pages to use instead of the switch default HTML pages.

**Step 1**
To specify the use of your custom authentication proxy web pages, first store your custom HTML files on the switch flash memory. To copy your HTML files to the switch flash memory, run the following command on the switch:

```
copy tftp/ftp flash
```
Step 2  After copying your HTML files to the switch, perform the following commands in global configuration mode:

<table>
<thead>
<tr>
<th></th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td><code>ip admission proxy http login page file device:login-filename</code></td>
<td>Specifies the location in the switch memory file system of the custom HTML file to use in place of the default login page. The device: is flash memory.</td>
</tr>
<tr>
<td>b.</td>
<td><code>ip admission proxy http success page file device:success-filename</code></td>
<td>Specifies the location of the custom HTML file to use in place of the default login success page.</td>
</tr>
<tr>
<td>c.</td>
<td><code>ip admission proxy http failure page file device:fail-filename</code></td>
<td>Specifies the location of the custom HTML file to use in place of the default login failure page.</td>
</tr>
<tr>
<td>d.</td>
<td><code>ip admission proxy http login expired page file device:expired-filename</code></td>
<td>Specifies the location of the custom HTML file to use in place of the default login expired page.</td>
</tr>
</tbody>
</table>

Step 3  Configure the customized authentication proxy web pages following the guidelines provided by the switch.

Step 4  Verify the configuration of a custom authentication proxy web page, as shown in the following example:

```
Switch# show ip admission configuration
Authentication proxy webpage
Login page : flash:login.htm
Success page : flash:success.htm
Fail Page : flash:fail.htm
Login expired Page : flash:expired.htm
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

Device Registration WebAuth Process

Using Device Registration Web Authentication (Device Registration WebAuth) and the Hotspot Guest portal, you can allow guest devices to connect to a private network without requiring usernames and passwords.

In this scenario, the guest connects to the network with a wireless connection. See Figure 38: Wireless Device Registration Web Authentication Flow for an example of the Device Registration WebAuth process flow. The following is an outline of the subsequent Device Registration WebAuth process, which is similar for both wireless and wired connections:

1. The network access device (NAD) sends a redirect to the Hotspot Guest portal.
2. If the MAC address of the guest device is not in any endpoint identity group or is not marked with an Acceptable Use Policy (AUP) accepted attribute set to true, Cisco ISE responds with a URL redirection specified in an authorization profile.
3. The URL redirection presents the guest with an AUP page (if enabled) when the guest attempts to access any URL.
   - If the guest accepts the AUP, the endpoint associated with their device MAC address is assigned to the configured endpoint identity group. This endpoint is now marked with an AUP accepted attribute set to true, to track the guest acceptance of the AUP.
   - If the guest does not accept the AUP or if an error occurs, for instance, while creating or updating the endpoint, an error message displays.

4. Based on the Hotspot Guest portal configuration, a post-access banner page (if enabled) with additional information may appear.

5. After the endpoint is created or updated, a Change of Authorization (CoA) termination is sent to the NAD.

6. After the CoA, the NAD re-authenticates the guest connection with a new MAC Auth Bypass (MAB) request. The new authentication finds the endpoint with its associated endpoint identity group, and returns the configured access to the NAD.

7. Based on the Hotspot Guest portal configuration, the guest is directed to the URL to which they requested access, or to a custom URL specified by the administrator, or to an Authentication Success Page.

The CoA type for both wired and wireless is Termination CoA. You can configure the Hotspot Guest portal to perform VLAN DHCP Release (and renew), thereby re-authorizing the CoA type for both wired and wireless to Change of Auth.

VLAN DHCP Release support is available for Mac OS and Windows on desktop devices only. It is not available for mobile devices. If the device being registered is mobile and the VLAN DHCP Release option is enabled, the guest is requested to manually renew their IP address. For mobile device users, we recommend using Access Control Lists (ACLs) on the WLC, rather than using VLANs.

*Figure 38: Wireless Device Registration Web Authentication Flow*
Support Device Access

- Personal Devices on a Corporate Network (BYOD), on page 495
- Personal Device Portals, on page 496
- Support Device Registration Using Native Supplicants, on page 502
- Device Portals Configuration Tasks, on page 503
- Manage Personal Devices Added by Employees, on page 516
- Monitor My Devices Portals and Endpoints Activity, on page 517

Personal Devices on a Corporate Network (BYOD)

When supporting personal devices on a corporate network, you must protect network services and enterprise data by authenticating and authorizing users (employees, contractors, and guests) and their devices. Cisco ISE provides the tools you need to allow employees to securely use personal devices on a corporate network.

Guests can automatically register their devices when logging in to Guest portals. Guests can register additional devices up to the maximum limit that you define in their guest type. These devices are registered into endpoint identity groups based on the portal configuration.

Guests can add their personal devices to the network by running the native supplicant provisioning (Network Setup Assistant), or by adding their devices to the My Devices portal. You can create native supplicant profiles, which determine the proper native supplicant provisioning wizard to use, based on the operating system.

Because native supplicant profiles are not available for all devices, users can use the My Devices portal to add these devices manually; or you can configure BYOD rules to register these devices.

ISE Community Resource

How To: ISE and BYOD - Onboarding, Registering, and Provisioning
How To: ISE and BYOD - Using Certificates for Differentiated Access

End-User Device Portals in a Distributed Environment

Cisco ISE end-user web portals depend on the Administration, Policy Services, and Monitoring personas to provide configuration, session support, and reporting.

- **Administration** Node—Configuration changes that you make to users, devices, and end-user portals are written to the Administration node.
Global Settings for Device Portals

Choose Work Centers > BYOD > Settings > Employee Registered Devices or Administration > Device Portal Management > Settings.

You can configure the following general settings for the BYOD and My Devices portals:

- Employee Registered Devices—Enter the maximum number of devices that an employee can register. By default, this value is set to 5 devices.
- Retry URL—Enter a URL that can be used to redirect the device back to Cisco ISE in Retry URL for onboarding.

Once you configure these general settings, they apply to all BYOD and My Devices portals that you set up for your company.

Related Topics
- Limit the Number of Personal Devices Registered by Employees, on page 502
- Provide a URL to Reconnect with BYOD Registration, on page 503
- End-User Device Portals in a Distributed Environment, on page 495

Personal Device Portals

Cisco ISE provides several web-based portals to support employee-owned personal devices. These Device portals do not participate in the guest or sponsor portal flows.

Use these portals to:

- Blacklist Portal—Provide information about personal devices that are “blacklisted” and cannot be used to gain access to the network.
- BYOD Portals—Enable employees to register their personal devices using native supplicant provisioning functionality.
- Certificate Provisioning Portal—Enables administrators and employees to request for user/device certificate(s) for devices that cannot go through the BYOD flow.
- Client Provisioning Portals—Force employees to download a posture agent on their devices that checks for compliance.
- MDM Portals—Enable employees to enroll their mobile devices with an external Mobile Device Management (MDM) system.
• **My Devices Portals**—Enable employees to add and register personal devices, including those that do not support native supplicant provisioning, and then manage them.

Cisco ISE provides you with the ability to host multiple device portals on the Cisco ISE server, including a predefined set of default portals. The default portal themes have standard Cisco branding that you can customize through the Admin portal. You can also choose to further customize a portal by uploading images, logos, and cascading style sheets (CSS) files that are specific to your organization.

## Access Device Portals

**Step 1**  
To access any of the Device portals, you can either:

- Click **Administration > Device Portal Management**. The **Configure and Customize Device Portals** page displays the list of supported Device portals.
- Choose **Administration > Device Portal Management**. The supported Device portals display in the drop-down menu.

**Step 2**  
Select the specific device portal that you want to configure.

## Blacklist Portal

Employees do not access this portal directly, but are redirected to it.

If employees lose their personal device or it is stolen, they can update its status in the My Devices portal, which adds it to the Blacklist endpoint identity group. This prevents others from using the device to obtain unauthorized network access. If anyone attempts to connect to the network using one of these devices, they are redirected to the Blacklist portal which informs them that the device is denied access to the network. If the device is found, employees can reinstate it (in the My Devices portal) and regain network access without having to register the device again. Depending on whether the device was lost or stolen, additional provisioning may be required before the device can be connected to the network.

You can configure the port settings (default is port 8444) for the Blacklist portal. If you change the port number, make sure it is not being used by another end-user portal.

For information about configuring a Blacklist portal, see **Edit the Blacklist Portal**, on page 507.

## Certificate Provisioning Portal

Employees can access the Certificate Provisioning portal directly.

The Certificate Provisioning portal allows employees to request certificates for devices that cannot go through the onboarding flow. For example, devices such as point-of-sale terminals cannot go through the BYOD flow and need to be issued certificates manually. The Certificate Provisioning portal allows a privileged set of users to upload a certificate request for such devices, generate key pairs (if required), and download the certificate.

Employees can access this portal and request for a single certificate or make a bulk certificate request using a CSV file.

---

**ISE Community Resource**

**Bring Your Own Device Portal**

Employees do not access this portal directly.

Employees are redirected to the Bring Your Own Device (BYOD) portal when registering personal devices using native supplicants. The first time employees attempt to access the network using a personal device, they may be prompted to manually download and launch the Network Setup Assistant (NSA) wizard and be guided through registering and installing the native supplicant. After they have registered a device, they can use the My Devices portal to manage it.

---

**Note**

BYOD flow is not supported when a device is connected to a network using AnyConnect Network Access Manager (NAM).

---

**Related Topics**

- Create a BYOD Portal, on page 509
- Personal Devices on a Corporate Network (BYOD), on page 495

**Client Provisioning Portal**

Employees do not access this portal directly, but are redirected to it.

The Client Provisioning system provides posture assessments and remediations for devices that are attempting to gain access to your corporate network. When employees request network access using their devices, you can route them to a Client Provisioning portal and require them to first download the posture agent. The posture agent scans the device for compliance, such as verifying that virus protection software is installed on it and that its operating system is supported.

---

**Related Topics**

- Create a Client Provisioning Portal, on page 511

**Mobile Device Management Portal**

Employees do not access this portal directly, but are redirected to it.

Many companies use a Mobile Device Management (MDM) system to manage employees’ mobile devices. Cisco ISE allows integration with external MDM systems that employees can use to enroll their mobile device and gain access to your corporate network. Cisco provides an external MDM interface that employees can enroll in to register their devices and then connect to the network.

The MDM portal enables employees to enroll in an external MDM system.

Employees can then use the My Devices portal to manage their mobile devices, such as lock their devices with a pin code, reset their device to its default factory settings, or remove applications and settings that were installed when registering the device.

Cisco ISE allows you to have a single MDM portal for all external MDM systems, or a portal for each individual MDM system.
For information about configuring MDM servers to work with ISE, see Create an MDM Portal, on page 512.

My Devices Portal

Employees can access the My Devices portal directly.

Some network devices that need network access are not supported by native supplicant provisioning and cannot be registered using the BYOD portal. However, employees can add and register personal devices, whose operating systems are not supported or do not have web browsers (such as printers, Internet radios, and other devices), using the My Devices portal.

Employees can add and manage new devices by entering the MAC address for the device. When employees add devices using the My Devices portal, Cisco ISE adds the devices to the Endpoints page as members of the RegisteredDevices endpoint identity group (unless already statically assigned to a different endpoint identity group). The devices are profiled like any other endpoint in Cisco ISE and go through a registration process for network access.

When two MAC addresses from one device are entered into the My Devices Portal by a user, profiling determines that they have the same hostname, and they are merged together as a single entry in ISE. For example, a user registers a laptop with wired and wireless addresses. Any operations on that device, such as delete, acts on both addresses.

When a registered device is deleted from the portal, the Device Registration Status and BYOD Registration Status attributes change to NotRegistered and No, respectively. However, these attributes remain unchanged when a guest (who is not an employee) registers a device using the Guest Device Registration page in the credentialed Guest portals, because these are BYOD attributes used only during employee device registration.

Regardless of whether employees register their devices using the BYOD or the My Devices portals, they can use the My Devices portal to manage them.

Note
The My Devices portal is not available when the Administrator's portal is down.

Related Topics
Create a My Devices Portal, on page 514

BYOD Deployment Options and Status Flow

The BYOD deployment flows that support personal devices vary slightly based on these factors:

- Single or dual SSID—With single SSID, the same WLAN is used for certificate enrollment, provisioning, and network access. In a dual SSID deployment, there are two SSIDs: one provides enrollment and provisioning, and the other provides secure network access.

- Windows, MacOS, iOS, or Android device—The native supplicant flow starts similarly, regardless of the device type, by redirecting employees using a supported personal device to the BYOD portal to confirm their device information. The process diverges based on device type.

Employee Connects to Network

1. Employee Credentials Are Authenticated—Cisco ISE authenticates the employee against the corporate Active Directory or other corporate identity stores and provides an authorization policy.
2. **Device Is Redirected to the BYOD Portal**—The device is redirected to the BYOD portal. The device’s MAC address field is automatically preconfigured, and the user can add a device name and description.

3. **Native Supplicant Is Configured (MacOS, Windows, iOS, Android)**—The native supplicant is configured; but the process varies by device:
   - MacOS and Windows devices—Employee clicks **Register** in the BYOD portal to download and install the supplicant provisioning wizard (Network Setup Assistant), which configures the supplicant and provides the certificate (if necessary) used for EAP-TLS certificate-based authentication. The issued certificate is embedded with the device's MAC address and employee's username.

   **Note**
   Network Setup Assistant cannot be downloaded to a Windows device, unless the user of that device has administrative privileges. If you cannot grant end users administrative privileges, then use your GPO to push the certificate to the user's device, instead of using the BYOD flow.

   - iOS devices—The Cisco ISE policy server sends a new profile using Apple’s iOS over the air to the iOS device, which includes:
     - The issued certificate (if configured) is embedded with the iOS device's MAC address and employee's username.
     - A Wi-Fi supplicant profile that enforces the use of EAP-TLS for 802.1X authentication.

   - Android devices—Cisco ISE prompts and routes employee to download the Cisco Network Setup Assistant (NSA) from the Google Play store. After installing the app, the employee can open NSA and start the setup wizard, which generates the supplicant configuration and issued certificate used to configure the device.

4. **Change of Authorization Issued**—After the user goes through the onboarding flow, Cisco ISE initiates a Change of Authorization (CoA). This causes the MacOS X, Windows, and Android devices to reconnect to the secure 802.1X network. For single SSID, iOS devices also connect automatically, but for dual SSID, the wizard prompts iOS users to manually connect to the new network.

   **Note**
   You can configure a BYOD flow that does not use supplicants. See the Cisco ISE Community document [https://supportforums.cisco.com/blog/12705471/ise-byod-registration-only-without-native-supplicant-or-certificate-provisioning](https://supportforums.cisco.com/blog/12705471/ise-byod-registration-only-without-native-supplicant-or-certificate-provisioning).

   **Note**
   Check the **Enable if Target Network is Hidden** check box only when the actual Wi-Fi network is hidden. Otherwise, Wi-Fi network configuration may not be provisioned properly for certain iOS devices, especially in the single SSID flow (where the same Wi-Fi network/SSID is used for both onboarding and connectivity).

**BYOD Session Endpoint Attribute**

The state of the endpoint attribute **BYODRegistration** changes during the BYOD flow to the following states.
Device Registration Status Endpoint Attribute

The state of the endpoint attribute `DeviceRegistrationStatus` changes during device registration to the following states:

- **Registered**—The device has been through BYOD flow, and it is registered. There is a 20-minute delay before the attribute changes from pending to registered.
- **Pending**—The device has been through BYOD flow, and it is registered. But, ISE has not seen it on the network.
- **Not Registered**—The device has not been through BYOD flow. This is the default state of this attribute.
- **Stolen**—The user logs onto the MyDevices portal, and marks a currently onboarded device as Stolen. When this happens:
  - If the device was onboarded by provisioning a certificate and a profile, ISE revokes the certificate that was provisioned to the device, and assigns the device’s mac address to the Blacklist identity group. That device no longer has network access.
  - If the device was onboarded by provisioning a profile (no certificate), ISE assigns the device to the Blacklist endpoint identity group. The device will still have network access, unless you create an authorization policy for this situation. For example, `IF Endpoint Identity Group is Blacklist AND BYOD_is_Registered THEN DenyAccess`.

An Administrator performs an action that disables network access for several devices, such as deleting or revoking a certificate.

If a user reinstates a stolen device, the status reverts to `not registered`. The user must delete that device, and add that it back. That starts the onboarding process.

- **Lost**—The user logs on to the MyDevices portal, and marks a currently onboarded device as Lost. That causes the following actions:
  - That device is assigned to Blacklist identity group.
  - Certificates provisioned to the device are not revoked.
  - The device status is updated to Lost.
  - “BYODRegistration” is updated to No.

A lost device still has network access unless you create an authorization policy to block lost devices. You can use the Blacklist identity group or the `endpoint:BYODRegistration` attribute in your rule. For example, `IF Endpoint Identity Group is Blacklist AND EndPoints:BYODRegistrations Equals No THEN BYOD`. For more granular access, you can also add `NetworkAccess:EAPAuthenticationMethod Equals PEAP or EAP-TLS or EAP-FAST”, InternalUser:IdentityGroup Equals <<group>>` to the IF part of the rule.
**Limit the Number of Personal Devices Registered by Employees**

You can allow employees to register between 1 and 999 personal devices. Regardless of the portal that employees used to register their personal devices, this setting defines the maximum number of devices registered across all portals.

**Step 1**  Choose Administration > Device Portal Management > Settings > Employee Registered Devices.

**Step 2**  Enter the maximum number of devices that an employee can register in **Restrict employees to**. By default, this value is set to 5 devices.

**Step 3**  Click **Save**. If you do not want to save any updates you made to the settings, click **Reset** to revert to the last saved values.

**Support Device Registration Using Native Supplicants**

You can create native supplicant profiles to support personal devices on the Cisco ISE network. Based on the profile that you associate with a user’s authorization requirements, Cisco ISE provides the necessary supplicant provisioning wizard to set up the user’s personal device to access the network.

The first time employees attempt to access the network using a personal device, they are guided automatically through registration and supplicant configuration. After they have registered the device, they can use the My Devices portal to manage their devices.

**Operating Systems Supported by Native Supplicants**

Native supplicants are supported for these operating systems:

- Android (excluding Amazon Kindle, B&N Nook)
- Mac OS X (for Apple Mac computers)
- Apple iOS devices (Apple iPod, iPhone, and iPad)
- Microsoft Windows 7, 8 (excluding RT), Vista, and 10

**Allow Employees to Register Personal Devices Using Credentialed Guest Portals**

Employees using credentialed Guest portals can register their personal devices. The self-provisioning flow supplied by the BYOD portal enables employees to connect devices to the network directly using native supplicants, which are available for Windows, MacOS, iOS, and Android devices.

**Before you begin**

You must create the native supplicant profiles.

**Step 1**  Choose Work Centers > Guest Access > Portals & Components > Guest Portals.
Step 2  Choose the credentialed Guest portal that you want to allow employees to use to register their devices using native supplicants and click Edit.

Step 3  On the Portal Behavior and Flow Settings tab and in BYOD Settings, check Allow employees to use personal devices on the network.

Step 4  Click Save and then Close.

Provide a URL to Reconnect with BYOD Registration

You can provide information that enables employees, who encounter a problem while registering their personal devices using the BYOD portal to reconnect with the registration process.

Step 1  Choose Administration > Device Portal Management > Settings > Retry URL.

Step 2  Change the IP address or enter a URL that can be used to redirect the device back to Cisco ISE in Retry URL for onboarding.

When the employee’s device encounters a problem during the registration process, it tries to reconnect to the Internet automatically. At this point, the IP address or domain name that you enter here redirects the device to Cisco ISE, which reinitiates the onboarding process. The default value is 1.1.1.1.

Step 3  Click Save. If you do not want to save any updates you made to the settings, click Reset to revert to the last saved values.

Device Portals Configuration Tasks

You can use a default portal and its default settings such as certificates, endpoint identity group, identity source sequence, portal themes, images, and other details provided by Cisco ISE. If you do not want to use the default settings, you should create a new portal or edit an existing one to meet your needs. You can duplicate a portal if you want to create multiple portals with the same settings.

After creating a new portal or editing a default one, you must authorize the portal for use. Once you authorize a portal for use, any subsequent configuration changes you make are effective immediately.

You do not need to authorize the My Devices portal for use.

If you choose to delete a portal, you must first delete any authorization policy rules and authorization profiles associated with it or modify them to use another portal.

Use this table for the tasks related to configuring the different Device portals.

<table>
<thead>
<tr>
<th>Task</th>
<th>Blacklist Portal</th>
<th>BYOD Portal</th>
<th>Client Provisioning Portal</th>
<th>MDM Portal</th>
<th>My Devices Portal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Policy Services, on page 504</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
<tr>
<td>Add Certificates, on page 505</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
<td>Required</td>
</tr>
</tbody>
</table>
Enable Policy Services

To support the Cisco ISE end-user web portals, you must enable portal-policy services on the node on which you want to host them.

Step 1 Choose Administration > System > Deployment
Step 2 Click the node and click Edit.
Step 3 On the General Settings tab, check Policy Service.
### Add Certificates

If you do not want to use the default certificates, you can add a valid certificate and assign it to a certificate group tag. The default certificate group tag used for all end-user web portals is Default Portal Certificate Group.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Chose Administration &gt; System &gt; Certificates &gt; System Certificates.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Add a system certificate and assign it to a certificate group tag that you want to use for the portal. This certificate group tag will be available to select during portal creation or editing.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose Administration &gt; Device Portal Management &gt; (any portals) &gt; Create or Edit &gt; Portal Settings.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select the specific certificate group tag from the Certificate Group Tag drop-down list that is associated with the newly added certificate.</td>
</tr>
</tbody>
</table>

### Create External Identity Sources

Cisco ISE can connect with external identity sources such as Active Directory, LDAP, RADIUS Token, and RSA SecurID servers to obtain user information for authentication and authorization. External identity sources also include certificate authentication profiles that you need for certificate-based authentications.

To work with passive identity services, which enable you to receive and share authenticated user identities, see Additional Passive Identity Service Providers, on page 368.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; Identity Management &gt; External Identity Sources.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Choose one of these options:</td>
</tr>
<tr>
<td></td>
<td>• Certificate Authentication Profile for certificate-based authentications.</td>
</tr>
<tr>
<td></td>
<td>• Active Directory to connect to an Active Directory as an external identity source See Active Directory as an External Identity Source, on page 323 for more details.</td>
</tr>
<tr>
<td></td>
<td>• LDAP to add an LDAP identity source. See LDAP, on page 409 for more details.</td>
</tr>
<tr>
<td></td>
<td>• RADIUS Token to add a RADIUS Token server. See RADIUS Token Identity Sources, on page 423 for more details.</td>
</tr>
<tr>
<td></td>
<td>• RSA SecurID to add an RSA SecurID server. See RSA Identity Sources, on page 428 for more details.</td>
</tr>
<tr>
<td></td>
<td>• SAML Id Providers to add an identity provider (IdP), such as Oracle Access Manager. See SAMLv2 Identity Provider as an External Identity Source, on page 433 for more details.</td>
</tr>
<tr>
<td></td>
<td>• Social Login to add a Social Login, such as Facebook, as an external identity source, see Social Login for Self-Registered Guests, on page 456.</td>
</tr>
</tbody>
</table>
Create Identity Source Sequences

Before you begin

Ensure that you have configured your external identity sources in Cisco ISE.

To perform the following task, you must be a Super Admin or System Admin.

For allowing guest users to authenticate through Local WebAuth, you must configure both the Guest Portal authentication source and the identity source sequence to contain the same identity stores.

Step 1  Choose Administration > Identity Management > Identity Source Sequences > Add.
Step 2  Enter a name for the identity source sequence. You can also enter an optional description.
Step 3  Check the Select Certificate Authentication Profile check box and choose a certificate authentication profile for certificate-based authentication.
Step 4  Choose the database or databases that you want to include in the identity source sequence in the Selected List box.
Step 5  Rearrange the databases in the Selected list in the order in which you want Cisco ISE to search the databases.
Step 6  Choose one of the following options in the Advanced Search List area:

- Do not access other stores in the sequence and set the AuthenticationStatus attribute to ProcessError — If you want Cisco ISE to discontinue the search, if the user is not found in the first selected identity source.

- Treat as if the user was not found and proceed to the next store in the sequence — If you want Cisco ISE to continue searching the other selected identity sources in sequence, if the user is not found in the first selected identity source.

While processing a request, Cisco ISE searches these identity sources in sequence. Ensure that you have the identity sources in the Selected list box listed in the order in which you want Cisco ISE to search them.

Step 7  Click Submit to create the identity source sequence that you can then use in policies.

Create Endpoint Identity Groups

Cisco ISE groups endpoints that it discovers into the corresponding endpoint identity groups. Cisco ISE comes with several system-defined endpoint identity groups. You can also create additional endpoint identity groups from the Endpoint Identity Groups page. You can edit or delete the endpoint identity groups that you have created. You can only edit the description of the system-defined endpoint identity groups; you cannot edit the name of these groups or delete them.

Step 1  Choose Administration > Identity Management > Groups > Endpoint Identity Groups.
Step 2  Click Add.
Step 3  Enter the name for the endpoint identity group that you want to create (do not include spaces in the name of the endpoint identity group).
Step 4  Enter the description for the endpoint identity group that you want to create.
Step 5  Click the Parent Group drop-down list to choose an endpoint identity group to which you want to associate the newly created endpoint identity group.
Step 6  Click Submit.

Edit the Blacklist Portal

Cisco ISE provides a single Blacklist portal that displays information when a lost or stolen device that is blacklisted in Cisco ISE is attempting to access your corporate network.

You can only edit the default portal settings and customize the default message that displays for the portal. You cannot create a new Blacklist portal, or duplicate or delete the default portal.

Before you begin

Ensure that you have the required certificates configured for use with this portal.

Step 1  Choose Administration > Device Portal Management > Blacklist Portal > Edit.

Step 2  Provide a unique Portal Name and a Description for the portal.

   Ensure that the portal name that you use here is not used for any other end-user portals.

Step 3  Use the Languages menu to export and import language files to use with the portal.

Step 4  Update the default values for certificate group tags, languages and so on in Portal Settings, and define behavior that applies to the overall portal.

   • HTTPS port—Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you modify this page. If you modify this page, update the port setting to comply with this restriction.

   If you assign Ports used by a non-guest (such as My Devices) portal to a guest portal, an error message displays.

   For posture assessments and remediation only, the Client Provisioning portal also uses Ports 8905 and 8909. Otherwise, it uses the same Ports assigned to the Guest portal.

   Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

   • Valid combinations include, using the Sponsor portal as an example:

      • Sponsor portal: Port 8443, Interface 0, Certificate tag A and My Devices portal: Port 8443, Interface 0, Certificate group A.

      • Sponsor portal: Port 8443, Interface 0, Certificate group A and My Devices portal: Port 8445, Interface 0, Certificate group B.

      • Sponsor portal: Port 8444, Interface 1, Certificate group A and Blacklist portal: Port 8444, Interface 0, Certificate group B.

   • Invalid combinations include:

      • Sponsor portal: Port 8443, Interface 0, Certificate group A and My Devices portal: 8443, Interface 0, Certificate group B.

      • Sponsor portal: Port 8444, Interface 0, Certificate tag A and Blacklist portal: Port 8444, Interface 0, Certificate group A.
• **Allowed interfaces** — Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed Port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets.

These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.

• The Ethernet interfaces must use IP addresses on different subnets.

• The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.

• The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP.

• Configure `ip host x.x.x.x yyy.domain.com` in ISE CLI to map secondary interface IP to FQDN, which is used to match Certificate Subject Name / Alternate Subject Name.

• If only the bonded NIC is selected - When the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN logs an error and exits. The PSN will NOT try to start the portal on the physical interface.

• **NIC teaming** or bonding is an O/S configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based on the portal settings configuration:

  • If both physical NICs and the corresponding bonded NIC are configured - When the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

• **Certificate group tag** — Pick a certificate group tag that specifies the certificate to use for the portal’s HTTPS traffic.

• **Display Language**

  • **Use browser locale** — Use the language specified in the client browser's locale setting as the display language of the portal. If browser locale's language is not supported by ISE, then the Fallback Language is used as the language portal.

  • **Fallback language** — Choose the language to use when language cannot be obtained from the browser locale, or if the browser locale language is not supported by ISE.

  • **Always use** — Choose the display language to use for the portal. This setting overrides the User browser locale option.

SSIDs available to sponsors — Enter the names or the SSIDs (Session Service Identifiers) of the networks that a sponsor can notify guests as the correct networks to connect to for their visit.

**Step 5** On the **Portal Page Customization** tab, customize the page title and message text that appears in the portal when an unauthorized device is attempting to gain access to the network.

**Step 6** Click **Save** and then **Close**.
Create a BYOD Portal

You can provide a Bring Your Own Device (BYOD) portal to enable employees to register their personal devices, so that registration and supplicant configuration can be done before allowing access to the network.

You can create a new BYOD portal, or you can edit or duplicate an existing one. You can delete any BYOD portal, including the default portal provided by Cisco ISE.

Any changes that you make to the Page Settings on the Portal Behavior and Flow Settings tab are reflected in the graphical flow in the device portal flow diagram. If you enable a page, such as the Support Information page, it appears in the flow and the employee will experience it in the portal. If you disable it, it is removed from the flow.

Before you begin

Ensure that you have the required certificates and endpoint identity groups configured for use with this portal.

---

**Step 1** Choose Administration > Device Portal Management > BYOD Portals > Create, Edit or Duplicate.

**Step 2** Provide a unique Portal Name and a Description for the portal.

Ensure that the portal name that you use here is not used for any other end-user portals.

**Step 3** Use the Language File drop-down menu to export and import language files to use with the portal.

**Step 4** Update the default values for ports, certificate group tags, endpoint identity groups and so on in Portal Settings, and define behavior that applies to the overall portal.

**Step 5** Update the Support Information Page Settings to help employees provide information that the Help Desk can use to troubleshoot network access issues.

**Step 6** On the Portal Page Customization tab, customize the Content Area message text that appears on the following pages during the provisioning process:

- **BYOD Welcome page:**
  - Device Configuration Required—When the device is redirected to the BYOD portal for the first time and requires certificate provisioning.
  - Certificate Needs Renewal—When the previous certificate needs to be renewed.

- **BYOD Device Information page:**
  - Maximum Devices Reached—When the maximum limit of devices that an employee can register is reached.
  - Required Device Information—When requesting device information that is required to enable an employee to register the device.

- **BYOD Installation page:**
  - Desktop Installation—When providing installation information for a desktop device.
  - iOS Installation—When providing installation instructions for an iOS mobile device.
  - Android Installation—When providing installation instructions for an Android mobile device

- **BYOD Success page:**
  - Success—When the device is configured and automatically connected to the network.
- Success: Manual Instructions—When the device is successfully configured and an employee must manually connect to the network.
- Success: Unsupported Device—When an unsupported device is allowed to connect to the network.

**Step 7**  
Click **Save** and then **Close**.

---

**What to do next**

You must authorize the portal in order to use it. You can also customize your portal either before or after you authorize it for use.

---

**Create a Certificate Provisioning Portal**

Cisco ISE provides a Certificate Provisioning portal that allows you to request for certificates for devices that cannot go through the onboarding flow. For example, devices such as point-of-sale terminals. You can request for a single certificate or make a bulk certificate request using a CSV file.

You can edit the default portal settings and customize the messages that appear on the portal. You can also create, duplicate, and delete the Certificate Provisioning portal.

There are two types of users who can access the Certificate Provisioning portal:

- Internal or external users with administrative privileges—Can generate certificate(s) for themselves as well as for others.
- All other users—Can generate certificate(s) only for themselves.

Users (network access users) who are assigned the Super Admin or ERS Admin role have access to this portal and can request certificates for others. However, if you create a new internal admin user and assign the Super Admin or ERS Admin role, the internal admin user will not have access to this portal. You must first create a network access user and then add the user to the Super Admin or ERS Admin group. Any existing network access users who are added to the Super Admin or ERS Admin group will have access to this portal.

To create an administrator account to access the Certificate Provisioning portal:

1. Add an internal user (Administration > Identity Management > Identities > Users > Add).
2. Add the user to the Super Admin or ERS Admin group (Administration > Admin Access > Administrators > Admin Users > Add > Select from existing network access user). The user is now both an internal network access user and a Super Admin or ERS Admin user.

For other users to be able to access the portal and to generate certificates for themselves, configure the Certificate Provisioning Portal Settings (Administration > Device Portal Management > Certificate Provisioning Portal > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Portal Settings). Ensure that you choose the appropriate identity source or identity source sequence under **Authentication Method** and choose the user group under **Configure Authorized Groups**. All users who belong to the groups that you choose will have access to the portal and can generate certificates for themselves.

**Before you begin**

Ensure that you have the required certificates configured for use with this portal.
Step 1  Choose Administration > Device Portal Management > Certificate Provisioning Portal > Create.
Ensure that the portal name that you use here is not used for any other end-user portals.

Step 2  Provide a unique Portal Name and a Description for the portal.

Step 3  Use the Language File menu to export and import language files to use with the portal

Step 4  Update the default values for certificate group tags, languages and so on in Portal Settings, and define behavior that applies to the overall portal.

Step 5  On the Portal Page Customization tab, customize the page title and message text that appears in the portal.

Step 6  Click Save and then Close.

Create a Client Provisioning Portal

You can provide a Client Provisioning portal to enable employees to download either the Cisco AnyConnect posture component or the Cisco NAC agent, which verifies the posture compliance of the device before allowing access to the network.

You can create a new Client Provisioning portal, or you can edit or duplicate an existing one. You can delete any Client Provisioning portal, including the default portal provided by Cisco ISE.

Users (network access users) who are assigned the Super Admin or ERS Admin role have access to this portal. However, if you create a new internal admin user and assign the Super Admin or ERS Admin role, the internal admin user will not have access to this portal. You must first create a network access user and then add the user to the Super Admin or ERS Admin group. Any existing network access users who are added to the Super Admin or ERS Admin group will have access to this portal.

To create an administrator account to access the Client Provisioning portal:

1. Add an internal user (Administration > Identity Management > Identities > Users > Add).
2. Add the user to the Super Admin or ERS Admin group (Administration > Admin Access > Administrators > Admin Users > Add > Select from existing network access user). The user is now both an internal network access user and a Super Admin or ERS Admin user.

For other users to be able to access the portal and to generate certificates for themselves, configure the Client Provisioning Portal Settings (Administration > Device Portal Management > Client Provisioning > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Portal Settings). Ensure that you choose the appropriate identity source or identity source sequence under Authentication Method and choose the user group under Configure Authorized Groups. All users who belong to the groups that you choose will have access to the portal.

Any changes that you make to the Page Settings on the Portal Behavior and Flow Settings tab are reflected in the graphical flow in the device portal flow diagram. If you enable a page, such as the Support Information page, it appears in the flow and the employee will experience it in the portal. If you disable it, it is removed from the flow.

Before you begin

Ensure that you have the required certificates and client provisioning policies configured for use with this portal.
Create an MDM Portal

You can provide a Mobile Device Management (MDM) portal to enable employees to manage their mobile devices that are registered for use on your corporate network.
You can create a new MDM portal, or you can edit or duplicate an existing one. You can have a single MDM portal for all of your MDM systems or you can create a portal for each system. You can delete any MDM portal, including the default portal provided by Cisco ISE. The default portal is for third-party MDM providers.

You can create a new MDM portal, or you can edit or duplicate an existing one. You can delete any MDM portal, including the default portal provided by Cisco ISE. The default portal is for third-party MDM providers.

Any changes that you make to the Page Settings on the Portal Behavior and Flow Settings tab are reflected in the graphical flow in the device portal flow diagram. If you enable a page, such as the Support Information page, it appears in the flow and the employee will experience it in the portal. If you disable it, it is removed from the flow.

Before you begin

Ensure that you have the required certificates and endpoint identity groups configured for use with this portal.

---

**Step 1** Choose **Administration > Device Portal Management > MDM Portals > Create, Edit or Duplicate.**

**Step 2** Provide a unique **Portal Name** and a **Description** for the portal.

Ensure that the portal name that you use here is not used for any other end-user portals.

**Step 3** Use the **Language File** drop-down menu to export and import language files to use with the portal.

**Step 4** Update the default values for ports, certificate group tags, endpoint identity groups and so on in **Portal Settings**, and define behavior that applies to the overall portal.

**Step 5** Update the following settings that apply to each of the specific pages:

- **Employee Mobile Device Management Settings**, access the link provided to configure third-party MDM providers and then define the acceptance policy behavior for employees using the MDM portals.

- **Support Information Page Settings** to help guests provide information that the Help Desk can use to troubleshoot network access issues.

**Step 6** On the **Portal Page Customization** tab, customize the **Content Area** messages that appears in the MDM portal during the device enrollment process:

- Unreachable—When the selected MDM system cannot be reached.
- Non-compliant—When the device being enrolled is not compliant with the requirements of the MDM system.
- Continue—When the device should try connecting to the network in case of connectivity issues.
- Enroll—When the device requires the MDM agent and needs to be enrolled in the MDM system.

**Step 7** Click **Save** and then **Close**.

---

**What to do next**

You must authorize the portal in order to use it. You can also customize your portal either before or after you authorize it for use. Also see the following topics:

- **Add Certificates**, on page 505
- **Create Endpoint Identity Groups**, on page 506
- **Create Authorization Profiles**, on page 515
Create a My Devices Portal

You can provide a My Devices portal to enable employees to add and register their personal devices that do not support native supplicants and cannot be added using the Bring Your Own Device (BYOD) portal. You can then use the My Devices portal to manage all devices that have been added using either portal.

You can create a new My Devices portal, or you can edit or duplicate an existing one. You can delete any My Devices portal, including the default portal provided by Cisco ISE.

Any changes that you make to the Page Settings on the Portal Behavior and Flow Settings tab are reflected in the graphical flow in the device portal flow diagram. If you enable a page, such as the Support Information page, it appears in the flow and the employee will experience it in the portal. If you disable it, it is removed from the flow.

Before you begin

Ensure that you have the required certificates, external identity stores, identity source sequences, and endpoint identity groups configured for use with this portal.

Step 1
Choose Administration > Device Portal Management > My Devices Portals > Create, Edit or Duplicate.

Step 2
Provide a unique Portal Name and a Description for the portal.

Step 3
Use the Language File drop-down menu to export and import language files to use with the portal.

Step 4
Update the default values for ports, certificate group tags, identity source sequences, endpoint identity groups, and so on in Portal Settings, and define behavior that applies to the overall portal.

Step 5
Update the following settings that apply to each of the specific pages:

• Login Page Settings—Specify employee credential and login guidelines.
• Acceptable Use Policy (AUP) Page Settings—Add a separate AUP page and define the acceptable use policy behavior for employees.
• Post-Login Banner Page Settings—Notify employees of additional information after they log into the portal.
• Employee Change Password Settings—Allow employees to change their own passwords. This option is enabled only if the employee is part of the Internal Users database.

Step 6
In the Portal Page Customization tab, customize the following information that appears in the My Devices portal during registration and management:

• Titles, instructions, content, field and button labels
• Error messages and notification messages

Step 7
Click Save and then Close.

What to do next

You can customize the portal if you want to change its appearance. See

• Customize Device Portals, on page 516
Create Authorization Profiles

When you authorize a portal, you are setting up the network authorization profiles and rules for network access.

Before you begin

You must create a portal before you can authorize it.

Step 1
Set up a special authorization profile for the portal.

Step 2
Create an authorization policy rule for the profile.

Create Authorization Profiles

Each portal requires that you set up a special authorization profile for it.

Before you begin

If you do not plan to use a default portal, you must first create the portal so you can associate the portal name with the authorization profile.

Step 1

Step 2
Create an authorization profile using the name of the portal that you want to authorize for use.

What to do next

You should create a portal authorization policy rule that uses the newly created authorization profile.

Create Authorization Policy Rules

To configure the redirection URL for a portal to use when responding to the users' (guests, sponsors, employees) access requests, define an authorization policy rule for that portal.

The url-redirect takes the following form based on the portal type, where:

- \( \text{ip:port} \) = the IP address and port number
- \( \text{PortalID} \) = the unique portal name

For a Hotspot Guest portal:

https://ip:port/guestportal/gateway?sessionID=SessionIdValue&portal=PortalID&action=cwa&type=drw
For a Mobile Device Management (MDM) portal:
https://ip:port/mdmportalgateway?sessionID=SessionIdValue&portal=PortalID&action=mdm

**Step 1** Choose **Policy** > **Policy Sets** to create a new authorization policy rule under **Standard** policies.

**Step 2** For **Conditions**, select an endpoint identity group that you want to use for the portal validation. For example, for the Hotspot Guest portal, select the default **GuestEndpoints** endpoint identity group and, for the MDM portal, select the default **RegisteredDevices** endpoint identity group.

**Note** Because the Hotspot Guest portal only issues a Termination CoA, do not use Network Access:UseCase EQUALS Guest Flow as one of the validation conditions in the Guest authorization policy. Instead, match the Identity Group that the endpoint belongs to for validation. For example,

- If "GuestEndpoint" + Wireless MAB then Permit Access
- If Wireless MAB then HotSpot Redirect

**Step 3** For **Permissions**, select the portal authorization profile that you created.

### Customize Device Portals

You can customize the portal appearance and user (guests, sponsors, or employees as applicable) experience by customizing the portal themes, changing UI elements on the portal pages, and editing error messages and notifications that display to the users. For more information about customizing portals, see **Customization of End-User Web Portals**, on page 519.

### Manage Personal Devices Added by Employees

When employees register a device using the Bring Your Own Device (BYOD) or the My Devices portals, it displays in the Endpoints list. Although employees can disassociate a device from their account by deleting it, the device remains in the Cisco ISE database. As a result, employees might need your assistance in resolving errors they encounter when working with their devices.

### Display Devices Added by an Employee

You can locate devices added by a specific employee using the Portal User field displayed on the Endpoints listing page. This might be useful if you need to delete devices registered by a specific user. By default, this field does not display, so you must enable it first before searching.

**Step 1** Choose **Work Centers** > **Network Access** > **Identities** > **Endpoints**.

**Step 2** Click the **Settings** icon and choose **Columns**.

**Step 3** Select **Portal User** to display this information in the Endpoints listing.

**Step 4** Click the **Show** drop-down list and choose **Quick Filter**.

**Step 5** Enter the user’s name in the **Portal User** field to display only the endpoints that are assigned to that particular user.
Errors When Adding Devices to My Devices Portal

Employees cannot add a device that was already added by another employee, and that device is still in the endpoints database.

If employees attempt to add a device that already exists in the Cisco ISE database:

• And it supports native supplicant provisioning, we recommend adding the device through the BYOD portal. This overwrites any registration details that were created when it was initially added to the network.

• If the device is a MAC Authentication Bypass (MAB) device, such as a printer, then first resolve ownership of the device. If appropriate, you can remove the device from the endpoints database using the Admin portal, so that the new owner can successfully add the device using the My Devices portal.

Note
The My Devices portal is not available when the Administrator's portal is down.

Devices Deleted from My Devices Portal Remain in Endpoints Database

When an employee deletes a device from the My Devices portal, the device is removed from the employee’s list of registered devices, but the device remains in the Cisco ISE endpoints database and displays in the Endpoints list.

To permanently delete the device from the Endpoints page, choose Work Centers > Network Access > Identities > Endpoints.

Limit the Number of Personal Devices Registered by Employees

You can allow employees to register between 1 and 999 personal devices. Regardless of the portal that employees used to register their personal devices, this setting defines the maximum number of devices registered across all portals.

Step 1 Choose Administration > Device Portal Management > Settings > Employee Registered Devices.
Step 2 Enter the maximum number of devices that an employee can register in Restrict employees to. By default, this value is set to 5 devices.
Step 3 Click Save. If you do not want to save any updates you made to the settings, click Reset to revert to the last saved values.

Monitor My Devices Portals and Endpoints Activity

Cisco ISE provides various reports and logs that allow you to view endpoint and user management information and guest and sponsor activity. Some of the Cisco ISE 1.2 reports have been deprecated, but the information can be viewed in other reports.

You can run these reports either on demand or on a scheduled basis.
Step 1  Choose **Operations > Reports**.
Step 2  Under the Report Selector, expand the **Guest Access Reports** and **Endpoints and Users** selections to view the various guest, sponsor, and endpoint related reports.
Step 3  Select the report and choose the data with which you want to search using the **Filters** drop-down list.
You can use filters on username, portal name, device name, endpoint identity group and other such data.
Step 4  Select the **Time Range** during which you want to view the data.
Step 5  Click **Run**.

---

**My Devices Login and Audit Report**

The My Devices Login and Audit report is a combined report that tracks:

- Login activity by employees at the My Devices portal.
- Device-related operations performed by the employees in the My Devices portal.

This report is available at: **Operations > Reports > Guest Access Reports > My Devices Login and Audit.**

**Registered Endpoints Report**

The Registered Endpoints report provides information about all the endpoints that are registered by employees. This report is available at: **Operations > Reports > Endpoints and Users > Registered Endpoints.** You can run a query on the following: identity, endpoint ID, identity profile, and the like, and you can generate a report. For information on supplicant provisioning statistics and related data, see Viewing Client Provisioning Reports.

You can query the endpoint database for endpoints that are assigned to the RegisteredDevices endpoint identity group. You can also generate reports for specific users that have the Portal User attribute set to a non-null value.

The Registered Endpoints Report provides information about a list of endpoints that are registered through device registration portals by a specific user for a selected period of time.
End-User Portals

Cisco ISE provides web-based portals for three primary sets of end users:

- Guests who need to temporarily access your enterprise network using the Guest portals (Hotspot and credentialed Guest portals)
- Employees who are designated as sponsors who can create and manage guest accounts using the Sponsor portal.
- Employees who are using their personal devices on the enterprise network using the various non-guest portals such as the Bring Your Own Device (BYOD), Mobile Device Management (MDM), and My Devices portals.

Customization of End-User Web Portals

Cisco provides several default portals, and lets you edit, duplicate, and create extra portals. You can also fully customize the portal appearance and, therefore, the portal experience. You can customize each individual portal without affecting other portals.

You can customize various aspects of the portal interface that apply to the entire portal or to specific pages of the portal, such as:

- Themes, images, colors, banners, and footers
- Languages used for displaying portal text, error messages, and notifications
- Titles, content, instructions, and field and button labels
• Notifications sent to guests via email, SMS, and printer (applies only to the Self-Registered Guest and Sponsor portals)
• Error and informational messages displayed to users
• Custom fields to gather guest information specific to your needs (applies only to the Self-Registered Guest and Sponsor portals)
For more information about customizing web portals, see ISE Portal Builder and HowTo: ISE Web Portal Customization Options.
Customization Methods

There are several different ways to customize the end-user portals pages, which require different levels of knowledge.

- **Basic**—All modifications are done on the portal Customization page, where you can:
  - Upload banners and logos.
  - Change some colors (except for buttons).
  - Change the text on the screens, and the language used on the entire portal.

- **Intermediate**
  - Use the mini-editor to add HTML and Javascript.
  - Use the jQuery mobile theme roller to change the color of all page elements.

- **Advanced**
  - Manually modify properties and CSS files.

After you customize your portal, you can create multiple portals (of the same type) by duplicating it. For example, if you customized your Hotspot Guest portal for one business entity, you can duplicate it and make minor changes to create custom Hotspot Guest portals for other business entities.

Tips for Customizing Portals with the Mini Editors

- Long words in a mini-editor box may scroll off the screen area of the portal. To prevent this, use the HTML paragraph attribute style="word-wrap: break-word". For example:

  ```html
  <p style="word-wrap:break-word">
  thisisaverylonglineoftextthatwillexceedthewidthoftheplacethatyouwanttoputitsousethisstructure
  </p>
  ```

- When you use HTML or javascript to customize portal pages, make sure that you use valid syntax. The tags and code that you enter into a mini-editor is not validated by ISE. Invalid syntax may cause problems during the portal flow.

Portal Content Types

Cisco ISE provides a default set of portal themes that you can use “as is” or customize by using the existing CSS files as models to create new custom files. However, you can alter the appearance of the portals without using customized CSS files.

For instance, if you want to use unique corporate logos and banner images, you can simply upload and use these new image files. You can customize the default color scheme by changing the color of the different elements and areas of the portals. You can even choose the language in which you want to view the custom changes as you make them.

When you design images to replace the logos and banner, make the images as close to the following pixel size as you can:
Note that ISE resizes the images to fit the portal, but images that are too small may not look right after resizing.

To perform advanced customization, such as changing the page layout or adding video clips or advertisements to your portal pages, you can use your own custom CSS files.

These types of changes within a specific portal are applied globally to all the pages of that portal. Changes to the page layout can be applied either globally or to just one specific page in the portal.

**Portal Page Titles, Content, and Labels**

You can customize the titles, text boxes, instructions, field and button labels, and other visual elements that the guest views on the end-user web portal pages. While you are customizing the page, you can even edit the page settings dynamically.

These changes are applied only to the specific page that you are customizing.

### Basic Customization of Portals

Select a predefined theme that best suits your needs, and use most of its default settings. You can then do some basic customization, such as:

- **Modify the Portal Theme Colors**, on page 523
- **Change the Portal Icons, Images, and Logos**, on page 525
- **Update the Portal Banner and Footer Elements**, on page 525
- **Change the Portal Display Language**, on page 524
- **Change the Titles, Instructions, Buttons, and Label Text**, on page 526
- **Format and Style Text Box Content**, on page 526

You can **View Your Customization**, on page 530 as you make the updates.

### Modify the Portal Theme Colors

You can customize the default color scheme in the default portal themes and change the color of the different elements and areas of the portals. These changes apply to the entire portal that you are customizing.

If you plan to change the portal colors, be aware of the following:

- You cannot use this option to change the color scheme in any of the custom portal themes that you may have imported for use with this portal. You must edit the custom theme CSS file to change its color settings.
Step 1 Navigate to these portals:

- For Guest portals, choose Work Centers > Guest Access > Portals & Components > Configure > Guest Portals > Edit > Portal Page Customization.
- For Device portals, choose Administration > Device Portal Management > (any Portals) > Edit > Portal Page Customization.

Step 2 Select one of the default themes from the Portal Theme drop-down list.

Step 3 Click Tweaks to override some of the color settings in the selected default portal theme.

a) Change the color settings for the banner and page backgrounds, text, and labels.

b) If you want to revert to the theme’s default color scheme, click Reset Colors.

c) Click OK if you want to view the color changes in Preview.

Step 4 Click Save.

Change the Portal Display Language

You can choose the language in which you want to view the custom changes as you make them. This change applies to the entire portal that you are customizing.

Step 1 Navigate to these portals:

- For Device portals, choose Administration > Device Portal Management > (any Portals) > Edit > Portal Page Customization > Global Customization.

Step 2 From the View In drop-down list, choose the language in which you want to view the text while customizing the page.

The drop-down list includes all languages in the language file associated with the specific portal.

What to do next

Make sure that you update any changes made in the selected language while customizing the portal page into all the supported language properties files.
Change the Portal Icons, Images, and Logos

If you want to use unique corporate logos, icons, and banner images, you can simply replace the existing images by uploading your custom images. Supported image formats include .gif, .jpg, .jpeg, and .png. These changes apply to the entire portal that you are customizing.

Before you begin

To include images in the footer of the portal, for instance in an advertisement, you should be able to access an external server that has these images.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Navigate to these portals:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• For Guest portals, choose Work Centers &gt; Guest Access &gt; Portals &amp; Components &gt; Guest Portals &gt; Edit &gt; Portal Page Customization.</td>
</tr>
<tr>
<td></td>
<td>• For Device portals, choose Administration &gt; Device Portal Management &gt; (any Portals) &gt; Edit &gt; Portal Page Customization.</td>
</tr>
</tbody>
</table>

Step 2 Under Images, click any of the logos, icons, and image buttons and upload your custom images.

Step 3 Click Save.

Update the Portal Banner and Footer Elements

You can customize the information that appears in the banner and footer sections of every page in the portal. These changes apply to the entire portal that you are customizing.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Navigate to these portals:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• For Guest portals, choose Work Centers &gt; Guest Access &gt; Portals &amp; Components &gt; Guest Portals &gt; Edit &gt; Portal Page Customization.</td>
</tr>
<tr>
<td></td>
<td>• For Device portals, choose Administration &gt; Device Portal Management &gt; (any Portals) &gt; Edit &gt; Portal Page Customization.</td>
</tr>
</tbody>
</table>

Step 2 Change the Banner title that appears on every portal page.

Step 3 Include these links for the guests who use your portals:

- **Help**—Online help (provided for only the Sponsor and My Devices portals).
- **Contact**—Technical support (set up the Support Information page to enable this).

Step 4 Add a disclaimer or a copyright notice in the Footer Elements to appear on the bottom of every portal page.

Step 5 Click Save.
Change the Titles, Instructions, Buttons, and Label Text

You can update all the text that is displayed in the portal. Each UI element on the page that you are customizing has a minimum and maximum range for the number of characters that you can enter. When available in some of the text blocks, you can use a mini-editor to apply visual styling to the text. These changes apply only to the specific portal page you are customizing. These page elements are different for email, SMS, and print notifications.

Step 1 Navigate to these portals:

- For Guest portals, choose Work Centers > Guest Access > Portals & Components > Configure > Guest Portals > Edit > Portal Page Customization.
- For Device portals, choose Administration > Device Portal Management > (any Portsals) > Edit > Portal Page Customization.

Step 2 Under Pages, choose the page that you want to change.

Step 3 Under Page Customizations, update any of the displayed UI elements. All pages contain Browser Page Title, Content Title, Instructional Text, Content, and two Optional Content text blocks. The fields in the Content area are specific to each page.

Format and Style Text Box Content

Use the mini-editor that is available in the Instructional Text, Optional Content 1, and Optional Content 2 text boxes to do basic formatting of the text. These changes apply only to the specific portal pages that you are customizing.

Use the Toggle Full Screen button to increase and decrease the size of the text boxes as you work in them.

Step 1 Navigate to these portals:

- For Device portals, choose Administration > Device Portal Management > (any Portsals) > Edit > Portal Page Customization.

Step 2 Under Pages, choose the page that you want to change.

Step 3 Under Page Customizations, in the Instructional Text and Optional Content text blocks, you can:

- Change the font, size, and color of the text.
- Style the text as bold, italics, or underlined.
- Create bulleted and numbered lists.
You can also use the **Toggle HTML Source** button to view the HTML tags that were applied to the text that you formatted using the mini-editor.

---

**Variables for Portal Pages Customization**

The navigation paths for these portal page text boxes are:

- For Guest portals, choose **Work Centers** > **Guest Access** > **Portals & Components** > **Guest Portals** > **Edit** > **Portal Page Customization** > **Pages**.

- For Sponsor portals, choose **Work Centers** > **Guest Access** > **Portals & Components** > **Sponsor Portals** > **Edit** > **Portal Page Customization** > **Pages**.

- For Device portals, choose **Administration** > **Device Portal Management** > (any Portals) > **Edit** > **Portal Page Customization** > **Pages**.

Use these variables when creating templates for portal content and guest notifications to enable consistency in the information presented to the portal users (guests, sponsors, and employees). Substitute text with the variable names listed here for each of the portals in the **Instructional Text**, **Optional Content 1**, and **Optional Content 2** text boxes.

**Table 33: List of Variables for Guest Portals**

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Substitute with Variable Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access code</td>
<td>ui_access_code</td>
</tr>
<tr>
<td>Use to provide an access code to</td>
<td></td>
</tr>
<tr>
<td>guests using either email, text</td>
<td></td>
</tr>
<tr>
<td>or print notifications.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>BYOD IOS SSID</td>
<td>ui_byod_success_ios_ssid</td>
</tr>
<tr>
<td>Use to specify the network that</td>
<td></td>
</tr>
<tr>
<td>a device should connect to after</td>
<td></td>
</tr>
<tr>
<td>on-boarding in a dual SSID flow.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Provisioning Agent Type</td>
<td>ui_client_provision_agent_type</td>
</tr>
<tr>
<td>Use to specify the currently</td>
<td></td>
</tr>
<tr>
<td>configured agent in the client</td>
<td></td>
</tr>
<tr>
<td>provisioning policy, such as the</td>
<td></td>
</tr>
<tr>
<td>AnyConnect agent or the NAC agent.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Client Provisioning Agent URL</td>
<td>ui_client_provision_agent_url</td>
</tr>
<tr>
<td>Use to specify the download URL</td>
<td></td>
</tr>
<tr>
<td>for the posture agent.</td>
<td></td>
</tr>
</tbody>
</table>
### Variables for Portal Pages Customization

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Substitute with Variable Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Provisioning agent install minutes</td>
<td>ui_client_provision_install_agent_mins</td>
</tr>
<tr>
<td>Use to notify guests the amount of time (set by the remediation timer) in which they must complete the installation instructions on the Client Provisioning page. If guests do not complete the installation instructions before the timer expires, they must refresh the browser page and go through the login process again.</td>
<td></td>
</tr>
<tr>
<td>Company</td>
<td>ui_company</td>
</tr>
<tr>
<td>Email address</td>
<td>ui_email_address</td>
</tr>
<tr>
<td>End date and time</td>
<td>ui_end_date_time</td>
</tr>
<tr>
<td>First name</td>
<td>ui_first_name</td>
</tr>
<tr>
<td>Last name</td>
<td>ui_last_name</td>
</tr>
<tr>
<td>Location name</td>
<td>ui_location_name</td>
</tr>
<tr>
<td>Maximum registered devices</td>
<td>ui_max_reg_devices</td>
</tr>
<tr>
<td>Maximum simultaneous logins</td>
<td>ui_max_siml_login</td>
</tr>
<tr>
<td>Password</td>
<td>ui_password</td>
</tr>
<tr>
<td>Person being visited (email)</td>
<td>ui_person_visited</td>
</tr>
<tr>
<td>Phone number</td>
<td>ui_phone_number</td>
</tr>
<tr>
<td>Reason for visit</td>
<td>ui_reason_visit</td>
</tr>
<tr>
<td>SMS Provider</td>
<td>ui_sms_provider</td>
</tr>
<tr>
<td>SSID</td>
<td>ui_ssid</td>
</tr>
<tr>
<td>Use to specify the wireless network that a guest can use to connect to the network.</td>
<td></td>
</tr>
<tr>
<td>Start date and time</td>
<td>ui_start_date_time</td>
</tr>
<tr>
<td>Time left</td>
<td>ui_time_left</td>
</tr>
<tr>
<td>Username</td>
<td>ui_user_name</td>
</tr>
</tbody>
</table>

**Table 34: List of Variables for Sponsor Portals**

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Substitute with Variable Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest - Company</td>
<td>ui_guest_company</td>
</tr>
<tr>
<td>Guest - Email address</td>
<td>ui_guest_email_address</td>
</tr>
</tbody>
</table>
### Variables for Portal Pages Customization

#### Table 35: List of Variables for MDM Portals

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Substitute with Variable Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest - End date and time</td>
<td>ui_guest_end_date_time</td>
</tr>
<tr>
<td>Guest - First name</td>
<td>ui_guest_first_name</td>
</tr>
<tr>
<td>Guest - Last name</td>
<td>ui_guest_last_name</td>
</tr>
<tr>
<td>Guest - Location name</td>
<td>ui_guest_location_name</td>
</tr>
<tr>
<td>Guest - Maximum registered devices</td>
<td>ui_guest_max_reg_devices</td>
</tr>
<tr>
<td>Guest - Maximum simultaneous logins</td>
<td>ui_guest_max_siml_login</td>
</tr>
<tr>
<td>Guest - Password</td>
<td>ui_guest_password</td>
</tr>
<tr>
<td>Guest - Person being visited (email)</td>
<td>ui_guest_person_visited</td>
</tr>
<tr>
<td>Guest - Phone number</td>
<td>ui_guest_phone_number</td>
</tr>
<tr>
<td>Guest - Reason for visit</td>
<td>ui_guest_reason_visit</td>
</tr>
<tr>
<td>Guest - SMS Provider</td>
<td>ui_guest_sms_provider</td>
</tr>
<tr>
<td>Guest - SSID</td>
<td>ui_guest_ssid</td>
</tr>
</tbody>
</table>

Use to specify the wireless network that a guest can use to connect to the network.

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Substitute with Variable Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest - Start date and time</td>
<td>ui_guest_start_date_time</td>
</tr>
<tr>
<td>Guest - Time left</td>
<td>ui_guest_time_left</td>
</tr>
<tr>
<td>Guest - Username</td>
<td>ui_guest_user_name</td>
</tr>
</tbody>
</table>

#### Table 36: List of Variables for My Devices Portals

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Substitute with Variable Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyDevices - Vendor Name</td>
<td>ui_mdm_vendor_name</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Display Name</th>
<th>Substitute with Variable Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>MyDevices - Login Failure Rate Limit</td>
<td>$user_login_failure_rate_limit$</td>
</tr>
<tr>
<td>MyDevices - Max Devices to Register</td>
<td>ui_max_register_devices</td>
</tr>
</tbody>
</table>
### View Your Customization

You can view how your customization will display to the portal users (guests, sponsors, or employees).

**Procedure**

- Click **Portal test URL** to view your changes.

#### Note

The test portal does not support Radius sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on Radius sessions.

- Click **Preview** to dynamically view how your changes appear on various devices:
  - Mobile devices—View your changes under **Preview**.
  - Desktop devices—Click **Preview** and then **Desktop Preview**. A new tab opens, and all the changes that you make are displayed on this tab.

  If the changes are not displayed, click **Refresh Preview**. The portal displayed is only meant for viewing your changes; you cannot click buttons or enter data.

### Custom Portal Files

The custom portal files menu lets you upload your own files to the ISE server, which you can use to customize all user facing portals (except for the admin portal). The files you upload are stored on the PSN, and synchronized to all PSNs.

Supported file types are:

- .png, .gif, .jpg, .jpeg, .ico - For backgrounds, announcements, advertisements
- .htm, .html, .js, .json, .css, .m4a, .m4v, .mp3, .mp4, .mpeg, .ogg, .wav - For advanced customization, for example, the portal builder

File sizes are limited to:

- 20 MB per file
- 200 MB total of all files

The path column in the list of files displays the URL to the file on this server, which you can use to reference it outside the mini-editor. If the file is an image, when you click the link, it opens a new window that displays the image.
Uploaded files can be referenced by all portal types, except the admin portal, in the mini-editors under portal page customization. To insert the file into a mini-editor, click the *insert file* button on the toolbar. Toggle to the HTML Source view, and you will see the inserted file surrounded by the appropriate HTML tags.

You can also view the displayable uploaded files in your browser from outside of ISE, for testing. The URL is https://ise_ip:8443/portal/customFiles/filename.

**Advanced Customization of Portals**

If you do not want to use one of the default portal themes provided by Cisco ISE, you can customize the portal to suit your needs. To do so, you should have experience working with CSS and Javascript files and the jQuery Mobile ThemeRoller application.

You are not allowed to alter the default portal themes, but you can:

- **Export a Portal’s Default Theme CSS File**, on page 536, and use it as a base for creating a custom portal theme.

- **Create a Custom Portal Theme CSS File**, on page 536, by editing the default portal theme and saving it as a new file.

- **Import the Custom Portal Theme CSS File**, on page 546, and apply it to the portal.

Based on the extent of your expertise and requirements, you can perform various types of advanced customization, such as use predefined variables to enable consistency in displayed information, add advertisements to your portal pages, use HTML, CSS and Javascript code to customize your content, and modify the portal page layout.

**Configure Portal Customization**

Cisco ISE offers you the ability to customize the content that displays on your end-user portals using HTML and Javascript code in the text boxes on the different pages listed under Portal Page Customization.

**Step 1**  Choose Administration > System > Admin Access > Settings > Portal Customization.

**Step 2**  Verify that Enable portal customization with HTML is checked by default. This setting enables you to include HTML tags in the Instructional Text, Optional Content 1 and Optional Content 2 text boxes.

**Step 3**  Check Enable portal customization with HTML and Javascript if you want to do advanced JavaScript customization by including <script> tags in the Instructional Text, Optional Content 1 and Optional Content 2 text boxes.

**What to do next**

You can then access the various portals and enter HTML and Javascript code in the text boxes based on the option you enabled here.

**Portal Theme and Structure CSS Files**

If you have experience with working with CSS files, you can customize the default portal theme CSS files to alter the portal presentation and manipulate elements such as the page layout, colors, and fonts. Customizing
the CSS files provides you with flexibility and control in specifying the presentation characteristics, it enables you to share formatting across multiple pages, and it reduces the complexity and repetition in the structural content.

Cisco ISE end-user portals use two distinct types of CSS files: structure.css and theme.css. Every portal theme has its own theme.css file, but there is only one structure.css file per portal type; for example guest.structure.css for Guest portals, sponsor.structure.css for Sponsor Portals, and mydevices.structure.css for My Devices portals.

The structure.css provides the styling for the page layout and structure. It defines the positioning of elements on each page and also includes jQuery Mobile structure styles. You can only view the structure.css file, but you cannot edit it. However, when you change the page layout within theme.css files, import these files into the portal, and apply them, the most recent changes take priority over the structure.css styles.

The theme.css files specify styles such as fonts, button colors, and header background. You can export the theme.css files, change the theme settings, and import them to use as custom themes for your portal. Any page layout style changes made to the theme.css files take priority over the styles that are defined in the structure.css file.

You cannot alter any of the Cisco provided default portal theme.css files. However, you can edit the settings in the files and save them to a new custom theme.css file. You can make further edits to the custom theme.css file, but when you import it back into Cisco ISE, remember to use the same theme name you originally used for it. You cannot use two different theme names for the same theme.css file.

For example, you can use a default green theme.css file to create a new custom blue theme.css file and name it as Blue. You can then edit the blue theme.css file, but when you import it again, you must reuse the same Blue theme name. You cannot call it Red, since Cisco ISE checks for the relationship between a filename and its name and the uniqueness of the theme’s name. You can however edit the blue theme.css file, save it as red theme.css, import the new file, and name it as Red.

About Changing Theme Colors with jQuery Mobile

The color scheme of Cisco’s end-user portals is compatible with jQuery ThemeRoller. You can easily edit the colors for an entire portal using the ThemeRoller web site.

ThemeRoller color “swatches” each contain a unique color scheme, which defines the colors, textures, and font settings for the primary UI elements, such as toolbars, content blocks, buttons, list items, and font text-shadow. A color scheme also defines the settings for various interaction states of the buttons: normal, hover, and pressed.

Cisco uses three swatches:

• Swatch A—The default swatch.
• Swatch B—Defines emphasized elements, such as an Accept button.
• Swatch C—Defines critical elements such as alerts, error messages, invalid input fields, and delete buttons.

You cannot apply additional swatches, unless you add HTML code (to the Optional Content, for example) with elements that use the newly added swatches.

To edit the default Cisco-provided CSS files or create new files based on the CSS classes and structures defined in the default themes, use the required version of jQuery Mobile ThemeRoller (Release 1.3.2).
For additional information on swatches and themes in jQuery Mobile ThemeRoller, see “Theming Overview” in Creating a Custom Theme with ThemeRoller. Use the online help in jQuery Mobile ThemeRoller to learn how to download, import, and share your custom themes.

For tutorials on how to use HTML, CSS, and Javascript code to customize the text and content that appears on your portal pages, visit Code Academy.

**Example of a Theme That Shows Cisco Swatches**

To demonstrate how swatches are used, the default theme for the Guest Portal was edited in ThemeRoller to show the differences in color.

The following screen shows a guest portal logon error (swatch C) along with a button that takes an action from the user (swatch B), and the rest of the screen is Swatch A.
Change Theme Colors with jQuery Mobile

Before you begin

Make sure you are using version 1.3.2 of jQuery Mobile ThemeRoller. The version you are using is displayed in the top-left corner of the screen, as shown below.

---

**Step 1** Export an existing theme from the portal you wish to change by clicking the Configuration tab on the portal, then Advanced Customization > Export/Import Themes.

**Step 2** In the Custom Theming dialog, export the theme you want to update.

**Step 3** Open that theme in a text editor, select all, and copy.

**Step 4** Paste that text (CSS) into the jQuery web site's Import Theme box.

**Step 5** Make your changes in the jQuery Mobile web-based application.

**Step 6** Export the updated theme from the jQuery website (the export format is ZIP).

**Step 7** Unzip the updated theme, and extract the updated theme in themes folder to your PC. The name of the theme is the one you provided on the jQuery website.

**Step 8** Import the extracted CSS theme file into your portal in the portal configuration page's Custom Theming dialog.

You can switch back and forth between the old theme and the new theme by clicking the Portal Theme drop-down on the portal configuration page.
Location Based Customization

When guest accounts are created, you can associate them with a location and specify a Service Set Identifier (SSID) attribute. Both the location and SSID are available as CSS classes that you can use to apply different CSS styles to portal pages, based on the guest's location and SSID.

Note

This information applies only to the credentialed Guest portals after the guests log in.

For example:

- Guest location—When guests with accounts that have *San Jose* or *Boston* as their locations log into a credentialed Guest portal, one of these classes is available on every portal page: `guest-location-san-jose` or `guest-location-boston`.

- Guest SSID—For an SSID named *Coffee Shop Wireless*, the following CSS class is available on every portal page: `guest-ssid-coffee-shop-wireless`. This SSID is the one you specified on the guest account and not the SSID that the guests connected to when they logged in.

You can also specify locations when you add devices such as switches and Wireless LAN Controllers (WLCs) to a network. This location is also available as a CSS class that you can use to apply different CSS styles to portal pages depending on the network device's location.

For example, if a WLC is assigned to *Seattle* and guests are redirected to Cisco ISE from the Seattle-WLC, the following CSS class is available on every portal page: `device-location-my-locations-usa-seattle`.

Related Topics

- [Customize Greetings Based on Guest Location](#), on page 542

User Device Type Based Customization

Cisco ISE detects the type of client device (guest, sponsor, or employee) to access your company’s network or end-user web portals (Guest, Sponsor, and Device). It is detected either as a mobile device (Android, iOS, and so on) or a desktop device (Windows, MacOS, and so on). The device type is available as a CSS class that you can use to apply different CSS styles to portal pages based on the user’s device type.

When a user logs in to any of the Cisco ISE end-user web portals, the following class is available on their portal pages: `cisco-ise-mobile` or `cisco-ise-desktop`. 
Export a Portal’s Default Theme CSS File

You can download a default portal theme provided by Cisco and customize it to suit your needs. You can use it as a base for performing advanced customization.

Step 1 Navigate to these portals:
- For Device portals, choose Administration > Device Portal Management > (any Portals) > Edit > Portal Page Customization > Pages.

Step 2 From the Advanced Customization drop-down list, choose Export/Import Themes.

Step 3 In the Custom Theming dialog box, use the drop-down list to select the theme that you want to customize.

Step 4 Click Export Theme CSS to download a default theme.css file to customize.

Step 5 Click Save to save the file to your desktop.

Create a Custom Portal Theme CSS File

You can create a custom portal theme by customizing an existing default portal theme and saving the changes in a new portal theme.css file. You can modify the default theme settings and the swatches to make global changes to the selected portal.

Before you begin
- Download to your desktop the theme.css file from the portal that you want to customize.
- This task requires experience working with HTML, CSS, and Javascript code.
- Use Release 1.3.2 of jQuery Mobile ThemeRoller.

Step 1 Import the downloaded portal theme.css file contents into the jQuery Mobile ThemeRoller tool.

Tip You can View Your Customization, on page 547 as you make your changes.

Step 2 (Optional) Embed Links in Portal Content, on page 537
Step 3 (Optional) Insert Variables for Dynamic Text Updates, on page 537
Step 4 (Optional) Use Source Code to Format Text and Include Links, on page 538
Step 5 (Optional) Add an Image as an Advertisement, on page 539
Step 6 (Optional) Customize Greetings Based on Guest Location, on page 542
Step 7 (Optional) Customize Greetings Based on User Device Type, on page 543
Step 8  (Optional) Set Up Carousel Advertising, on page 540
Step 9  (Optional) Modify the Portal Page Layout, on page 544
Step 10  Save the customized file as a new theme.css file.

Note  You cannot save the edits to the default CSS theme files. You can only create new custom files with any edits you have made.

Step 11  When your new theme.css file is ready, you can import it into Cisco ISE.

---

**Embed Links in Portal Content**

You can add links to enable guests to access various websites from the portal pages. These changes apply only to the specific portal page that you are customizing.

Use the **Toggle Full Screen** button to increase and decrease the size of the text boxes as you work in them.

---

**Step 1**  Navigate to these portals:

- For Guest portals, choose Work Centers > Guest Access > Portals and Components > Guest Portals > Edit > Portal Page Customization.
- For Device portals, choose Administration > Device Portal Management > (any Portals) > Edit > Portal Page Customization.

**Step 2**  Under **Pages**, choose the page that you want to update.

**Step 3**  Under **Page Customizations**, use the mini-editor provided with the **Optional Content** text blocks to add links to portal pages.

**Step 4**  Click the **Create Link** button. A **Link Properties** dialog box displays.

**Step 5**  Enter the **URL** and the text you want to hyperlink in the **Description** window for the URL.

For the link to work correctly, include the protocol identifier in the URL. For example, use http://www.cisco.com instead of www.cisco.com.

**Step 6**  Click **Set** and then **Save**.

You can use the **Toggle HTML Source** button to view the HTML tags that were applied to the text that you formatted using the mini-editor.

---

**Insert Variables for Dynamic Text Updates**

You can also create templates for text displayed on the portal by substituting predefined variables ($variable$) that dynamically update the content. This enables consistency in the text and information that you display to guests. These changes apply only to the specific portal pages that you are customizing.
Use the `Toggle Full Screen` button to increase and decrease the size of the text boxes as you work in them.

**Step 1** Navigate to these portals:
- For Guest portals, choose `Work Centers > Guest Access > Portals and Components > Guest Portals > Edit > Portal Page Customization`.
- For Device portals, choose `Administration > Device Portal Management > (any Portals) > Edit > Portal Page Customization`.

**Step 2** Under `Pages`, choose the page you want to update.

**Step 3** Under `Page Customizations`, use the mini-editor provided with the `Instructional Text`, `Optional Content 1`, and `Optional Content 2` text boxes to create text templates for the portal pages.

For example, you can create a single welcome message template for multiple guests, but personalize the message that displays to the guests after they successfully log in and connect to the network.

**Step 4** Enter the information in the text boxes as you normally would.

For example, you could enter a welcome message for your portal:

```plaintext
Welcome to our company’s Guest portal,
```

**Step 5** At the point where you want to substitute a variable for the text, click the `Insert Variable` button. A list of variables appears in the pop-up menu.

**Step 6** Select the variable that you want to substitute in your text.

In this example, choose `First name` to display each guest’s first name in the welcome message. The variable `$ui_first_name$` is inserted at your cursor position:

```plaintext
Welcome to our company’s Guest portal,$ui_first_name$.
```

This is the welcome message that would appear on the portal welcome page for guests whose first name is John: `Welcome to our company’s Guest portal, John`.

**Step 7** Continue to use the list of variables as needed until you have completed entering the information in the text boxes.

**Step 8** Click `Save`.

You can use the `Toggle HTML Source` button to view the HTML tags that were applied to the text that you formatted using the mini-editor.

---

**Use Source Code to Format Text and Include Links**

Besides using the mini-editor’s formatting and link icons with plain text, you can also use HTML, CSS, and Javascript code to customize text that displays on the portal pages. These changes apply only to the specific portal pages that you are customizing.

Use the `Toggle Full Screen` button to increase and decrease the size of the text boxes as you work in them.
Before you begin

Ensure that Enable portal customization with HTML is enabled by default in Administration > System > Admin Access > Settings > Portal Customization.

Step 1
Navigate to these portals:

- For Device portals, choose Administration > Device Portal Management > (any Portals) > Edit > Portal Page Customization.

Step 2
Under Pages, choose the page that you want to update.

Step 3
Under Page Customizations, use the mini-editor provided with the Instructional Text, Optional Content 1, and Optional Content 2 text boxes to enter and view source code.

Step 4
Click the Toggle HTML Source button.

Step 5
Enter your source code.

For example, to underline your text, enter:

```html
<p style="text-decoration:underline;">Welcome to Cisco!</p>
```

For example, to include a link using HTML code, enter:

```html
<a href="http://www.cisco.com">Cisco</a>
```

Important When inserting an external URL in the HTML code, make sure that you enter the absolute (entire) URL path, including “http” or “https”.

Step 6
Click Save.

Related Topics

Configure Portal Customization, on page 531

Add an Image as an Advertisement

You can include images and advertisements to appear in specific areas of the portal pages.

Use the Toggle Full Screen button to increase and decrease the size of the text boxes as you work in them.

Before you begin

Ensure that Enable portal customization with HTML is enabled in Administration > System > Admin Access > Settings > Portal Customization.

Step 1
Navigate to these portals:

- For Device portals, choose Administration > Device Portal Management > (any Portals) > Edit > Portal Page Customization.

**Step 2** Under Pages, choose the page that you want to update.

**Step 3** Under Page Customizations, use the mini-editor provided with the Instructional Text, Optional Content 1, and Optional Content 2 text boxes to enter and view source code.

**Step 4** Click the Toggle HTML Source button.

**Step 5** Enter your source code.

For example, to include a product advertisement and its image using HTML code on the Hotspot Guest portal post-access banner, enter this code in the Optional Content 1 text box on the Post-Access Banner page:

```html
<p style="text-decoration:underline;">Optimized for 10/40/100 Campus Services!</p>
<img src="http://www.static-cisco.com/assets/prod/root/catalyst_6800.jpg" width="100%" />
```

**Note** When inserting an external URL in the HTML code, make sure that you enter the absolute (entire) URL path, including “http” or “https”.

*Figure 40: Sample Image for an Advertisement*

---

**Set Up Carousel Advertising**

Carousel advertising is an advertisement format in which several product images or text descriptions are displayed and rotate in a repeating loop within a banner. Use carousel advertising on your guest portals to promote several related products or a variety of different products offered by your company.

Use the Toggle Full Screen button to increase and decrease the size of the text boxes as you work in them.
Before you begin

Choose Administration > System > Admin Access > Settings > Portal Customization and check Enable portal customization with HTML and Javascript.

Step 1

Navigate to these portals:

- For Device portals, choose Administration > Device Portal Management > (any Portals) > Edit > Portal Page Customization.

Step 2

Under Pages, choose the page that you want to update.

Step 3

Under Page Customizations, use the mini-editor provided with the Instructional Text, Optional Content 1, and Optional Content 2 text boxes to enter and view source code.

Step 4

Click the Toggle HTML Source button.

Step 5

Enter your source code.

For example, to implement carousel advertising using product images on the Guest portals, enter the following HTML and Javascript code in the Optional Content 1 text box on the Post-Access Banner (for Hotspot portals) or Post Login Banner (for credentialed Guest portals) pages:

```html
<script>
var currentIndex = 0;
setInterval(changeBanner, 5000);

function changeBanner(){
  var div = document.getElementById("image-ads");
  if(div){
    currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
    div.innerHTML = bannersArray[currentIndex];
  }
}
</script>

<style>
.grey{
  color: black;
  background-color: lightgrey;
}
</style>

<div class="grey" id="image-ads">
</div>
```
For example, to implement carousel advertising using text product descriptions on the Guest portals, enter the following HTML and Javascript code in the Optional Content 2 text box on the Post-Access Banner (for Hotspot portals) or Post Login Banner (for credentialed Guest portals) pages:

```html
<script>
var currentIndex = 0;
setInterval(changeBanner, 2000);

function changeBanner(){
var bannersArray = ["Optimize branch services on a single platform while delivering an optimal application experience across branch and WAN infrastructure", "Transform your Network Edge to deliver high-performance, highly secure, and reliable services to unite campus, data center, and branch networks", "Differentiate your service portfolio and increase revenues by delivering end-to-end scalable solutions and subscriber-aware services"];
var colorsArray = ["grey", "blue", "green"]; 
var div = document.getElementById("text-ads");
if(div){
  currentIndex = (currentIndex<2) ? (currentIndex+1) : 0;
  div.innerHTML = bannersArray[currentIndex];
  div.className = colorsArray[currentIndex];
}
</script>

<style>
.grey{
  color: black;
  background-color: lightgrey;
}
.blue{
  color: black;
  background-color: lightblue;
}
.green{
  color: black;
  background-color: lightgreen;
}
</style>
<div class="grey" id="text-ads">
Optimize branch services on a single platform while delivering an optimal application experience across branch and WAN infrastructure
</div>

Note: When inserting an external URL in the HTML code, you must enter the absolute (entire) URL path, including “http” or “https”.

**Step 6**  Click Save.

---

**Customize Greetings Based on Guest Location**

This example shows how to customize the successful login message that your guests see after they log into a credentialed Guest portal (not Hotspot), based on the locations configured in their guest type.

Use the **Toggle Full Screen** button to increase and decrease the size of the text boxes as you work in them.

**Step 1**  Navigate to one of these portals:
• For Guest portals, choose Work Centers > Guest Access > Portals & Components > Guest Portals > Edit > Portal Page Customization.

Step 2 Under Pages, choose the Authentication Success page.
Step 3 Under Page Customizations, use the mini-editor provided with the Optional Content 1 text box to enter and view HTML source code.
Step 4 Click the Toggle HTML Source button.
Step 5 Enter your source code.

For example, to include a location-based greeting, enter this code in the Optional Content 1:

```html
<style>
.custom-greeting {
    display: none;
}
guest-location-san-jose .custom-san-jose-greeting {
    display: block;
}
guest-location-boston .custom-boston-greeting {
    display: block;
}
</style>
<div class="custom-greeting custom-san-jose-greeting">
    Welcome to The Golden State!
</div>
<div class="custom-greeting custom-boston-greeting">
    Welcome to The Bay State!
</div>
```

Guests will see a different message after successful logon, depending on their specific location.

### Customize Greetings Based on User Device Type

You can customize the greetings that you send to your users (guest, sponsor, or employee) after they log into any of the Cisco ISE end-user web portals (Guest, Sponsor and Device), based on their client device type (mobile or desktop).

Use the Toggle Full Screen button to increase and decrease the size of the text boxes as you work in them.

Step 1 Navigate to these portals:

• For Guest portals, choose Work Centers > Guest Access > Portals & Components > Guest Portals > Edit > Portal Page Customization.
• For Device portals, choose Administration > Device Portal Management > (any Portals) > Edit > Portal Page Customization.

Step 2 Under Pages, choose the page that you want to update.
Step 3 Under Page Customizations, use the mini-editor provided with the Optional Content 1 text box to enter and view HTML source code.
**Step 4** Click the **Toggle HTML Source** button.

**Step 5** Enter your source code.

For example, to include a device type-based greeting on the AUP page, enter this code in the **Optional Content 1** text box on the AUP page:

```html
<style>
  .custom-greeting {
    display: none;
  }
  .cisco-ise-desktop .custom-desktop-greeting {
    display: block;
  }
  .cisco-ise-mobile .custom-mobile-greeting {
    display: block;
  }
</style>
<div class="custom-greeting custom-mobile-greeting">
  Try our New Dark French Roast! Perfect on the Go!
</div>
<div class="custom-greeting custom-desktop-greeting">
  We brought back our Triple Chocolate Muffin! 
  Grab a seat and dig in!
</div>
```

Users will see a different greeting on the AUP page depending on the type of device they used to gain access to the network or portal.

---

**Modify the Portal Page Layout**

You can manipulate the overall layout of the pages; for example, you can add a sidebar to an AUP page that provides additional information or links to information.

**Step 1** Add the following CSS code to the bottom of the custom theme.css file that you create and plan to apply to your portal. This changes the AUP page layout so that the **Optional Content 1** text box appears as:

- A sidebar in the desktop device mode
- A sidebar in the mobile device mode

```css
#page-aup .cisco-ise-optional-content-1 {
  margin-bottom: 5px;
}
@media all and ( min-width: 60em ) {
  #page-aup .cisco-ise-optional-content-1 {
    float: left;
    margin-right: 5px;
    width: 150px;
  }
  #page-aup .cisco-ise-main-content {
    float: left;
    width: 800px;
  }
  #page-aup .cisco-ise-main-content h1,
  #page-aup .cisco-ise-main-content p {
    margin-right: auto;
    margin-left: -200px;
  }
```

---
You can then add links using HTML code in the **Optional Content 1** text box for the AUP page for that portal.

**Step 2**  
Navigate to these portals:

- For Guest portals, choose **Work Centers > Guest Access > Portal & Components > Guest Portals > Edit > Portal Page Customization**.
- For Sponsor portals, choose **Work Centers > Guest Access > Portal & Components > Sponsor Portals > Edit > Portal Page Customization**.
- For Device portals, choose **Administration > Device Portal Management > (any Portals) > Edit > Portal Page Customization**.

**Step 3**  
Under **Pages**, choose the page for which you want to include a side bar.

**Step 4**  
Under **Page Customizations**, use the mini-editor provided with the **Optional Content 1** text box to enter and view source code.

**Step 5**  
Click the **Toggle HTML Source** button.

**Step 6**  
Enter your source code.

For example, to include a side bar for the AUP page, enter this code in the **Optional Content 1** text box on the AUP page:

```html
<ul data-role="listview">
  <li>Rent a Car</li>
  <li>Top 10 Hotels</li>
  <li>Free Massage</li>
  <li>Zumba Classes</li>
</ul>
```

*Figure 41: View of a Side Bar on a Sample AUP Page (on a Desktop Device)*
Import the Custom Portal Theme CSS File

You can upload any custom theme.css file that you have created and apply it to any of your end-user portals. These changes apply to the entire portal that you are customizing.

Any time you edit a custom theme.css file and import it back into Cisco ISE, remember to use the same theme name you originally used for it. You cannot use two different theme names for the same theme.css file.

Step 1  Navigate to these portals:

- For Guest portals, choose Work Centers > Guest Access > Portals & Components > Configure > Guest Portals > Edit > Portal Page Customization.
- For Device portals, choose Administration > Device Portal Management > (any Portals) > Edit > Portal Page Customization.

Step 7  Click Save.

What to do next

You can customize other pages by entering different text or HTML code in the Optional Content text boxes.
Step 2 From the Advanced Customization drop-down list, choose Export/Import Themes.

Step 3 In the Custom Theming dialog box, click Browse to find your new theme.css file.

Step 4 Enter a Theme Name for the new file.

Step 5 Click Save.

What to do next
You can apply this custom portal theme to the portal that you want to customize.

1. Choose the updated theme from the Portal Themes drop-down list to apply to the entire portal.
2. Click Save.

Delete a Custom Portal Theme
You can delete any custom portal theme that you have imported into Cisco ISE, unless it is being used by one of your portals. You cannot delete any of the default themes provided by Cisco ISE.

Before you begin
The portal theme that you want to delete should not be used by any of the portals.

Step 1 Navigate to these portals:
• For Guest portals, choose Work Centers > Guest Access > Portals & Components > Guest Portals > Edit > Portal Page Customization.
• For Device portals, choose Administration > Device Portal Management > (any Portals) > Edit > Portal Page Customization.

Step 2 From the Advanced Customization drop-down list, choose Delete Themes.

Step 3 Select the portal theme that you want to delete from the Theme Name drop-down list.

Step 4 Click Delete and then Save.

View Your Customization
You can view how your customization will display to the portal users (guests, sponsors, or employees).

Procedure
• Click Portal test URL to view your changes.
The test portal does not support Radius sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on Radius sessions.

Note

- Click **Preview** to dynamically view how your changes appear on various devices:
  - Mobile devices—View your changes under **Preview**.
  - Desktop devices—Click **Preview** and then **Desktop Preview**. A new tab opens, and all the changes that you make are displayed on this tab.

If the changes are not displayed, click **Refresh Preview**. The portal displayed is only meant for viewing your changes; you cannot click buttons or enter data.

**Portal Language Customization**

The Guest, Sponsor, My Devices, and Client Provisioning portals are localized into all supported languages and locales. This includes text, labels, messages, field names, and button labels. If the client browser requests a locale that is not mapped to a template in Cisco ISE, the portals display content using the English template.

Using the Admin portal, you can modify the fields used for the Guest, Sponsor, and My Devices portals for each language individually, and you can add more languages. Currently, you cannot customize these fields for the Client Provisioning portal.

By default, each type of portal supports 15 languages. You select which language a portal uses, and optionally update page content for that language, on the Portal Page Customization page. Note, if you change fonts and content on the page for one language, those changes to not carry over into the other languages. The changes you make on the Portal Page Customization screen are included when you export the Language File.

The supported languages are:

- Chinese Simplified
- Chinese Traditional
- Czech
- Dutch
- English
- French
- German
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Portuguese
Note

NAC and MAC agent installers and WebAgent pages are not localized.

To Edit the Language Used by a Portal

1. Open the portal you want to edit.
2. On the Portal Page Customization tab, and near the top of the page, select the language you want to edit in the view in drop-down.
3. Change content, headings, and fonts as desired.
4. Save that portal configuration, and repeat this flow for the next languages you want to update.

To Edit the Language File

Each Portal Page Customization page also provides a Language File. The Language File is a ZIP of attribute files that you can use to customize headings and text that are part of the portal flow, but is not available to customize on the Portal Page Customization page.

The Language File also contains the mapping to the particular browser locale setting (for example, for French: fr, fr-fr, fr-ca) along with all of the string settings for the entire portal in that language. If you change the browser locale setting for one language, the change is applied to all the other end-user web portals. For example, if you change the French properties browser locale from fr,fr-fr,fr-ca to fr,fr-fr in the Hotspot Guest portal, the change is applied to the My Devices portal also.

You can export the zipped language file and make updates to it, including adding new languages or deleting existing ones you do not need.

For instructions about how to update the Language File, see:

- Export the Language File, on page 549
- Add or Delete Languages from the Language File, on page 550
- Import the Updated Language File, on page 551

Export the Language File

You can export the language file available for each portal type to edit and customize the existing values specified in it, and add or delete a language.

Note

Only some of the dictionary keys in the language properties files support HTML in their values (text).

Step 1

Navigate to these portals:
Add or Delete Languages from the Language File

If a language you want to use for your portal type is missing from the language file, you can create a new language properties file and add it to the zipped language file. If there are languages you do not need, you can delete their language properties files.

Before you begin

Export the zipped language file available with each portal type in order to add or delete language properties files.

Step 1

Use any editor that displays UTF-8 (such as Notepad++) to open the predefined language file for the portal type to which you want to add or delete languages.

If you want to add or delete languages for more than one portal type, use all the appropriate portal properties files.

Step 2

To add a new language, save an existing language properties file as the new language properties file using the same naming convention of the other files in the zipped language file. For example, to create a new Japanese language properties file, save the file as Japanese.properties (LanguageName.properties).

Step 3

Associate the new language with its browser locale by specifying the browser local value in the first line of the new language properties file. For example, LocaleKeys=ja,ja-jp (LocaleKeys=browser locale value) should be the first line in the Japanese.properties file.

Step 4

Update all the values (text) of the dictionary keys in the new language properties file.

You cannot change the dictionary keys; just their values.

Note

Only some of the dictionary keys support HTML in their values (text).

What to do next

1. Zip all the properties files (new and existing) and create a new zipped language file. Do not include any folders or directories.

Note

When using a Mac, extracting the ZIP file produces a DS store. When you compress the language file after editing, do not include the DS store in the ZIP. To learn methods of extracting the DS store, see https://superuser.com/questions/198569/compressing-folders-on-a-mac-without-the-ds-store.

2. Use a new name or its original name for the zipped language file.
3. Import the zipped language file into the specific portal you exported it from.

**Import the Updated Language File**

You can import an edited language file that you have customized by adding or deleting language properties files or by updating text in existing properties files.

**Note**

Ensure that you do not copy and paste customization content from Word files. Alternately, select File > Save As and save the Word file in HTML format. You can then copy and paste customization content from the HTML file.

**Step 1**

Navigate to these portals:

- For Guest portals, choose Work Centers > Guest Access > Portals & Components > Guest Portals > Edit.
- For Sponsor portals, choose Work Centers > Guest Access > Portals & Components > Sponsor Portals > Edit.
- For Device portals, choose Administration > Device Portal Management > (any Portals) > Edit.

**Step 2**

Click Language File and choose Import from the drop-down list.

**Step 3**

Browse to find the new zipped language file on your desktop.

**Step 4**

Import it back for the portal type from where you exported it.

**What to do next**

To display the changed text or the new language you added, select the specific language from the View In drop-down list.

**Customization of Guest Notifications, Approvals, and Error Messages**

Within in each portal, you can customize how guests receive notifications via email, SMS text messages, and print. Use these notifications to email, text, or print the login credentials:

- When guests use the Self-Registration Guest portal and successfully register themselves.
- When sponsors create guest accounts and want to provide the details to guests. When you create sponsor groups, you can determine whether to authorize sponsors to use SMS notifications. They can always use email and print notifications, if these facilities are available.

You can also customize email notifications to sponsors requesting that they approve a self-registering guest trying to gain access to the network. Additionally, you can customize the default error messages that display to guests and sponsors.
Customize Email Notifications

You can customize the information that is sent via email to guests.

Before you begin

- Configure the SMTP server to enable email notifications. Choose Administration > System > Settings > SMTP Server.
- Configure support for email notifications to guests. Choose Work Centers > Guest Access > Settings > Guest Email Settings. Check Enable email notifications to guests.
- Ensure that Enable portal customization with HTML is enabled by default in Administration > System > Admin Access > Settings > Portal Customization.

Step 1 For Self-Registered Sponsor portals, choose Work Centers > Guest Access > Portals & Components > Sponsor Portals > Edit > Portal Page Customization > Notify Guests > Email Notification.

Step 2 You can change the default Logo (Email) that was specified under Global Page Customizations.

Step 3 Specify the Subject and Email body. Use predefined variables to specify the guest account information to be included in the email message. Use the mini-editor and HTML tags to customize the text.

Step 4 Under Settings, you can:

- Send username and password separately in different emails. If you select this option, two separate tabs appear in Page Customizations for customizing the Username Email and Password Email notifications.
- Send Test Email to your email address to preview your customization on all devices to ensure that the information appears as it should.

Step 5 Click Save and then Close.

Customize SMS Text Message Notifications

You can customize the information that is sent via SMS text messages to guests.

Before you begin

- Configure the SMTP server, which is used to send emails to the SMS gateway to deliver the SMS text message. Choose Administration > System > Settings > SMTP Server.
- Configure the sponsor groups to support the SMS text notification.
- Set up an account with a third-party SMS gateway. Choose Administration > Systems > Settings > SMS Gateway. Cisco ISE sends the text messages as email messages to the gateway, which forwards the messages via the SMS provider to the specified user.
- Ensure that Enable portal customization with HTML is enabled by default in Administration > System > Admin Access > Settings > Portal Customization.
Step 1  For Self-Registered Guest or Sponsor portals, choose Work Centers > Guest Access > Portals & Components > Guest or Sponsor Portals > Edit > Portal Page Customization > SMS Receipt or SMS Notification.

Step 2  Use the mini-editor and HTML tags to customize the Message Text. Use predefined variables to specify the guest account information to be included in the SMS text message.

Step 3  Under Settings, you can:

- Send username and password separately in different text messages. If you select this option, two separate tabs appear in Page Customizations for customizing the Username Message and Password Message notifications.

- Send Test Message to a cell phone to preview your customization to ensure that the information appears as it should. The supported phone number formats include: +1 ###-###-####, ###-####, (###) ###-####, 1########## and so on.

Step 4  Click Save and then Close.

### Customize Print Notifications

You can customize the information that is printed for guests.

**Note**

Within each portal, the print notification logo is inherited from the email notification logo setting.

**Before you begin**

Ensure that Enable portal customization with HTML is enabled by default in Administration > System > Admin Access > Settings > Portal Customization.

Step 1  For Self-Registered Guest and Sponsor portals, choose Work Centers > Guest Access > Portals & Components > Guest or Sponsor Portals > Edit > Portal Page Customization > Print Receipt or Print Notification.

Step 2  Specify the Print Introduction Text. Use predefined variables to specify the guest account information to be included in the email message. Use the mini-editor and HTML tags to customize the text.

Step 3  Preview your customization in the thumbnail or click Print Preview. You cannot view any HTML customization in the thumbnail. If you select the Print Preview option, a window appears from which you can print the account details to ensure that the information appears as it should.

Step 4  Click Save and then Close.

### Customize Approval Request Email Notifications

You can require sponsors to approve self-registering guests before their accounts are created and before they can obtain their login credentials. You can customize the information that is sent via email to sponsors requesting their approval. This notification only displays if you have specified that self-registering guests using the Self-Registered Guest portals require approval before they are granted network access.
Before you begin

- Configure the SMTP server to enable email notifications. Choose Administration > Systems > Settings > SMTP Server.
- Configure support for email notifications to guests. Choose Work Centers > Guest Access > Settings > Guest Email Settings. Check Enable email notifications to guests.
- If you want a Sponsor to approve self-registered account requests, check Require self-registered guests to be approved under Self-Registration Page Settings on the Portal Behavior and Flow Settings tab. That enables the Approval Request Email tab under Notifications in Portal Page Customization, where you can customize the email that goes to the Sponsor.

Step 1
Choose Work Centers > Guest Access > Portals & Components > Configure > Self-Registered Guest Portals > Edit > Portal Page Customization > Approval Request Email. Here you can:

a) Change the default Logo that is specified under Global Page Customizations.

b) Specify the Subject and Email body. Use predefined variables to specify the guest account information to be included in the email message. Use the mini-editor and HTML tags to customize the text. For example, to include a link to the Sponsor portal in the request approval email, click the Create a Link button, add the FQDN to the Sponsor portal.

c) Preview your customization on all devices using Send Test Email to ensure that it appears as it should.

d) Don't forget to click Save and then Close.

Step 2
Customize the content of the approval email sent by the Sponsor. Choose Work Centers > Guest Access > Portals & Components > Sponsor Portals, choose Portal Page Customization, and then the Email Notification tab.

Edit Error Messages

You can fully customize the error messages that appear on the Failure pages displayed for guests, sponsors and employees. Failure pages are available with all end-user web portals, except the Blacklist portal.

Step 1
Do one of the following:

- For Device portals, choose Adminsitration > Device Portals Management > (any portals) > Edit > Portal Page Customizations > Messages > Error Messages.

Step 2
From the View In drop-down list, choose the language in which you want to view the text while customizing the messages. The drop-down list includes all the languages in the language file associated with a specific portal. Make sure that you update any changes made while customizing the portal page into the supported languages properties files.

Step 3
Update the error message text. You can search for specific error messages by typing in keywords such as aup to find AUP related error messages.

Step 4
Click Save and Close.
Enable and Configure Cisco ISE Services

- Set Up Policy Conditions, on page 557
- Manage Authentication Policies, on page 569
- Manage Authorization Policies and Profiles, on page 607
- Configure Threat Centric NAC Service, on page 619
- Configure Smart Licensing and Smart Call Home Services, on page 637
- Cisco ISE Endpoint Profiling Policies, on page 643
- Configure Client Provisioning, on page 737
- Configure Client Posture Policies, on page 771
- Cisco TrustSec Policies Configuration, on page 807
CHAPTER 19

Set Up Policy Conditions

- Policy Conditions, on page 557
- Simple and Compound Conditions, on page 557
- Policy Evaluation, on page 558
- Create Simple Conditions, on page 558
- Create Compound Conditions, on page 559
- Profiler Conditions, on page 560
- Posture Conditions, on page 561
- Create Patch Management Conditions, on page 565
- Create Disk Encryption Conditions, on page 565
- Network Conditions, on page 566
- Create Time and Date Conditions, on page 568

Policy Conditions

Cisco ISE is a policy-based, network-access-control solution, which offers the following services: network-access, guest, posture, client provisioning, and profiler services. While configuring Cisco ISE, you create authentication, authorization, guest, posture, and profiler policies. Policy conditions are basic building blocks of policies. There are two types of policy conditions, simple and compound.

This chapter describes the policy conditions and how you can create them for the various services that Cisco ISE offers.

Simple and Compound Conditions

Cisco ISE uses rule-based policies to provide network access, profiler, posture, and guest services. These rule-based policies consist of rules that are made up of conditions. Cisco ISE allows you to create conditions as individual, reusable policy elements that can be referred from other rule-based policies. There are two types of conditions:

- Simple condition—A simple condition consists of an operand (attribute), an operator (equal to, not equal to, greater than, and so on), and a value. You can save simple conditions and use them in other rule-based policies.

  Simple condition takes the form: A operand B, where A can be any attribute from the Cisco ISE dictionary and B can be one of the values that the attribute A can take. The Device Type is used as an attribute for
all network devices that can include all device types as its value, which means that A Equals B in the
following form:
DEVICE:Device Type Equals All Device Types

• Compound condition—A compound condition is made up of one or more simple conditions that are
connected by the AND or OR operator. Compound conditions are built on top of simple conditions. You
can save and reuse compound conditions in other rule-based policies.

Compound condition can take any one of the following forms:
• (X operand Y) AND (A operand B) AND (X operand Z) AND so on
• (X operand Y) OR (A operand B) OR (X operand Z) OR so on

where X and A are attributes from the Cisco ISE dictionary such as the username and device type.

This is an example of a compound condition:

You cannot delete conditions that are used in a policy or are part of a compound condition.

Policy Evaluation

Policies consist of rules, where each rule consists of conditions to be satisfied that allow actions to be performed
such as access to network resources. Rule-based conditions form the basis of policies, the sets of rules used
when evaluating requests.

At run-time, Cisco ISE evaluates the policy conditions and then applies the result that you define based on
whether the policy evaluation returns a true or a false value.

During policy-condition evaluation, Cisco ISE compares an attribute with a value. It is possible that where
the attribute specified in the policy condition may not have a value assigned in the request. In such cases, if
the operator that is used for comparison is “not equal to,” then the condition will evaluate to true. In all other
cases, the condition will evaluate to false.

For example, in the condition Radius.Calling_Station_ID Not Equal to 1.1.1.1, if the Calling Station ID is
not present in the RADIUS request, then this condition will evaluate to true. This evaluation is not unique to
the RADIUS dictionary and occurs because of the usage of the “Not Equal to” operator.

In ISE, the Policy Sets table provides a list of all policy sets currently configured in the system. The order of
the enabled policy sets determines the order by which the system searches for the relevant policy set every
time an endpoint requests access. The last row in the Policy Set table from the Policy page is the default policy
that will be applied if none of the rules match the request in any of the other configured policy sets. You can
edit the allowed protocols and identity source selection in default policy set, but you cannot delete it.

Create Simple Conditions

You can create simple conditions and reuse them when you define authentication, authorization, or guest
policies.
Before you begin

To perform the following task, you must be a Super Admin or Policy Admin.

---

Step 1: Choose Policy > Policy Elements > Conditions.

Step 2: Click the arrow next to Authentication or Authorization or Guest, and then click Simple Conditions.

Step 3: Click Add.

Step 4: Enter appropriate values for the Name, Description, Attribute, Operator, and Value fields.

If you specify any Identity Group in simple conditions, ensure that you represented them in FQDN form, like the following:

\[(\text{InternalUser}:\text{IdentityGroup}) : \text{Equal} : (\text{UserIdentityGroups}: \text{Identity Group Name})\]

Cisco ISE will not accurately resolve Identity Group entries in the following form: \[(\text{InternalUser}:\text{IdentityGroup}) : \text{Equal} : (\text{Identity Group Name})\]

Step 5: Click Submit to save the condition.

---

Related Topics

- Policy Evaluation, on page 558
- Simple and Compound Conditions, on page 557

---

Create Compound Conditions

You can create compound conditions and reuse them when you define authentication policies.

Before you begin

- Cisco ISE includes predefined compound conditions for some of the most common use cases. You can edit these predefined conditions to suit your requirements.
- To perform the following task, you must be a Super Admin or Policy Admin.

---

Step 1: Choose Policy > Policy Elements > Conditions.

Step 2: Click the arrow next to Authentication or Authorization or Guest and then click Compound Conditions.

Step 3: Click Add.

Step 4: Enter a name for the compound condition. You can enter an optional description.

Step 5: Click Select Existing Condition from Library to choose an existing simple condition or click Create New Condition to choose an attribute, operator, and value from the expression builder.

Step 6: Click the action icon at the end of this row to add more conditions.

Step 7: Click Add Attribute/Value to create a new condition or click Add Condition from Library to add an existing simple condition.

Step 8: Select operand from the drop-down list. You can choose AND or OR and the same operand will be used between all the conditions in this compound condition.

Step 9: Click Submit to create the compound condition.
Profiler Conditions

Profiler conditions are policy elements and are similar to other conditions. However unlike authentication, authorization, and guest conditions, the profiling conditions can be based on a limited number of attributes. The Profiler Conditions page lists the attributes that are available in Cisco ISE and their description.

Profiler conditions can be one of the following:

- **Cisco Provided**—Cisco ISE includes predefined profiling conditions when deployed and they are identified as Cisco Provided in the Profiler Conditions page. You cannot delete Cisco Provided profiling conditions. You can also find Cisco Provided conditions in the System profiler dictionaries in the following location: Policy > Policy Elements > Dictionaries > System.

  For example, MAC dictionary. For some products, the OUI (Organizationally Unique Identifier) is an unique attribute that you can use it first for identifying the manufacturing organization of devices. It is a component of the device MAC address. The MAC dictionary contains the MACAddress and OUI attributes.

- **Administrator Created**—Profiler conditions that you create as an administrator of Cisco ISE or predefined profiling conditions that are duplicated are identified as Administrator Created. You can create a profiler condition of DHCP, MAC, SNMP, IP, RADIUS, NetFlow, CDP, LLDP, and NMAP types using the profiler dictionaries in the Profiler Conditions page.

Although, the recommended upper limit for the number of profiling policies is 1000, you can stretch up to 2000 profiling policies.

Create a Profiler Condition

Endpoint profiling policies in Cisco ISE allow you to categorize discovered endpoints on your network, and assign them to specific endpoint identity groups. These endpoint profiling policies are made up of profiling conditions that Cisco ISE evaluates to categorize and group endpoints.

**Before you begin**

To perform the following task, you must be a Super Admin or Policy Admin.

**Step 1** Choose Policy > Policy Elements > Conditions > Profiling > Add.

**Step 2** Enter values for the fields as described in the Endpoint Profiling Policies Settings, on page 1085.

**Step 3** Click Submit to save the profiler condition.

**Step 4** Repeat this procedure to create more conditions.

**Related Topics**

Profiler Conditions, on page 560
Posture Conditions

A posture condition can be any one of the following simple conditions: a file, a registry, an application, a service, or a dictionary condition. One or more conditions from these simple conditions form a compound condition, which can be associated to a posture requirement.

When you deploy Cisco ISE on your network for the first time, you can download posture updates from the web for the first time. This process is called the initial posture update.

After an initial posture update, Cisco ISE also creates Cisco defined simple and compound conditions. Cisco defined simple conditions have pc_ as their prefixes and compound conditions have pr_ as their prefixes.

You can also configure Cisco ISE to download the Cisco-defined conditions periodically as a result of dynamic posture updates through the web. You cannot delete or edit Cisco defined posture conditions.

A user defined condition or a Cisco defined condition includes both simple conditions and compound conditions.

Simple Posture Conditions

You can use the Posture Navigation pane to manage the following simple conditions:

• File Conditions—A condition that checks the existence of a file, the date of a file, and the versions of a file on the client.

• Registry Conditions—A condition that checks for the existence of a registry key or the value of the registry key on the client.

• Application Conditions—A condition that checks if an application or process is running or not running on the client.

| Note | If a process is installed and running, user is compliant. However, the Application condition works in reverse logic; If an application is not installed and not running, the end user is complaint. If an application is installed and running, the end user is non-complaint. |

• Service Conditions—A condition that checks if a service is running or not running on the client.

• Dictionary Conditions—A condition that checks a dictionary attribute with a value.

• USB Conditions—A condition that checks for the presence of USB mass storage device.

Related Topics

File Condition Settings, on page 1092
Registry Condition Settings, on page 1097
Application Condition Settings, on page 1099
Service Condition Settings, on page 1101
Dictionary Simple Condition Settings, on page 1108
USB Condition Settings, on page 1114
Create Simple Posture Conditions

You can create file, registry, application, service, and dictionary simple conditions that can be used in posture policies or in other compound conditions.

Before you begin

To perform the following task, you must be a Super Admin or Policy Admin.

Step 1
Choose Policy > Policy Elements > Conditions > Posture.

Step 2
Choose any one of the following: File, Registry, Application, Service, or Dictionary Simple Condition.

Step 3
Click Add.

Step 4
Enter the appropriate values in the fields.

Step 5
Click Submit.

Compound Posture Conditions

Compound conditions are made up of one or more simple conditions, or compound conditions. You can make use of the following compound conditions while defining a Posture policy.

• Compound Conditions—Contains one or more simple conditions, or compound conditions of the type File, Registry, Application, or Service condition
• Antivirus Compound Conditions—Contains one or more AV conditions, or AV compound conditions
• Antispyware Compound Conditions—Contains one or more AS conditions, or AS compound conditions
• Dictionary Compound Conditions—Contains one or more dictionary simple conditions or dictionary compound conditions
• Antimalware Conditions—Contains one or more AM conditions.

Predefined Condition for Enabling Automatic Updates in Windows Clients

The pr_AutoUpdateCheck_Rule is a Cisco predefined condition, which is downloaded to the Compound Conditions page. This condition allows you to check whether the automatic updates feature is enabled on Windows clients. If a Windows client fails to meet this requirement, then the Network Access Control (NAC) Agents enforce the Windows client to enable (remediate) the automatic updates feature. After this remediation is done, the Windows client becomes posture compliant. The Windows update remediation that you associate in the posture policy overrides the Windows administrator setting, if the automatic updates feature is not enabled on the Windows client.

Preconfigured Antivirus and Antispyware Conditions

Cisco ISE loads preconfigured antivirus and antispyware compound conditions in the AV and AS Compound Condition pages, which are defined in the antivirus and antispyware support charts for Windows and Macintosh operating systems. These compound conditions can check if the specified antivirus and antispyware products exist on all the clients. You can also create new antivirus and antispyware compound conditions in Cisco ISE.
Antivirus and Antispyware Support Chart

Cisco ISE uses an antivirus and antispyware support chart, which provides the latest version and date in the definition files for each vendor product. Users must frequently poll antivirus and antispyware support charts for updates. The antivirus and antispyware vendors frequently update antivirus and antispyware definition files, look for the latest version and date in the definition files for each vendor product.

Each time the antivirus and antispyware support chart is updated to reflect support for new antivirus and antispyware vendors, products, and their releases, the NAC Agents receive a new antivirus and antispyware library. It helps NAC Agents to support newer additions. Once the NAC Agents retrieve this support information, they check the latest definition information from the periodically updated se-checks.xml file (which is published along with the se-rules.xml file in the se-templates.tar.gz archive), and determine whether clients are compliant with the posture policies. Depending upon what is supported by the antivirus and antispyware library for a particular antivirus, or antispyware product, the appropriate requirements will be sent to the NAC Agents for validating their existence, and the status of particular antivirus and antispyware products on the clients during posture validation.

The antivirus and antispyware support chart is available on Cisco.com.

Compliance Module

The compliance module contains a list of fields, such as vendor name, product version, product name, and attributes provided by OPSWAT that supports Cisco ISE posture conditions.

Vendors frequently update the product version and date in the definition files, therefore, you must look for the latest version and date in the definition files for each vendor product by frequently polling the compliance module for updates. Each time the compliance module is updated to reflect the support for new vendors, products, and their releases, the AnyConnect agents receive a new library. It helps AnyConnect agent to support newer additions. Once the AnyConnect agents retrieve this support information, they check the latest definition information from the periodically updated se-checks.xml file (which is published along with the se-rules.xml file in the se-templates.tar.gz archive), and determine whether clients are compliant with the posture policies. Depending upon what is supported by the library for a particular antivirus, antispyware, antimalware, disk encryption, or patch management product, the appropriate requirements will be sent to the AnyConnect agents for validating their existence, and the status of the particular products on the clients during posture validation.

The compliance module is available on Cisco.com.

Table given below lists the OPSWAT API versions that support and do not support the ISE posture policy. There are different policy rules for agents that support versions 3 and 4.

Table 37: OPSWAT API Versions

<table>
<thead>
<tr>
<th>Posture Condition</th>
<th>Compliance Module Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPSWAT</td>
<td></td>
</tr>
<tr>
<td>Antivirus</td>
<td>3.x or earlier</td>
</tr>
<tr>
<td>Antispyware</td>
<td>3.x or earlier</td>
</tr>
<tr>
<td>Antimalware</td>
<td>4.x or later</td>
</tr>
<tr>
<td>Disk Encryption</td>
<td>3.x or earlier and 4.x or later</td>
</tr>
<tr>
<td>Patch Management</td>
<td>3.x or earlier and 4.x or later</td>
</tr>
</tbody>
</table>
Create Compound Posture Conditions

You can create compound conditions that can be used in posture policies for posture assessment and validation.

Before you begin
To perform the following task, you must be a Super Admin or Policy Admin.

| Step 1 | Choose Policy > Policy Elements > Conditions > Posture > Compound Conditions > Add. |
| Step 2 | Enter appropriate values for the fields. |
| Step 3 | Click Validate Expression to validate the condition. |
| Step 4 | Click Submit. |

Related Topics
- Posture Conditions, on page 561
- Simple Posture Conditions, on page 561
- Compound Posture Conditions, on page 562
- Predefined Condition for Enabling Automatic Updates in Windows Clients, on page 562
- Preconfigured Antivirus and Antispyware Conditions, on page 562

Compliance Module Version

<table>
<thead>
<tr>
<th>Posture Condition</th>
<th>Compliance Module Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>USB</td>
<td>4.x or later</td>
</tr>
<tr>
<td>Non-OPSWAT</td>
<td>Any version</td>
</tr>
<tr>
<td>File</td>
<td>Any version</td>
</tr>
<tr>
<td>Application</td>
<td>Any version</td>
</tr>
<tr>
<td>Compound</td>
<td>Any version</td>
</tr>
<tr>
<td>Registry</td>
<td>Any version</td>
</tr>
<tr>
<td>Service</td>
<td>Any version</td>
</tr>
</tbody>
</table>

Note
- Be sure to create separate posture policies for version 3.x or earlier and version 4.x or later, in anticipation of clients that may have installed any one of the above versions.
- OESIS version 4 support is provided for compliance module 4.x and Cisco AnyConnect 4.3 and higher. However, AnyConnect 4.3 supports both OESIS version 3 and version 4 policies.
- Version 4 compliance module is supported by ISE 2.1 and higher.
Create Patch Management Conditions

You can create a policy to check the status of a selected vendor’s patch management product. For example, you can create a condition to check if Microsoft System Center Configuration Manager (SCCM), Client Version 4.x software product is installed at an endpoint.

**Note**

Supported versions of Cisco ISE and AnyConnect:
- Cisco ISE version 1.4 and later
- AnyConnect version 4.1 and later

**Before you begin**

To perform the following task, you must be a Super Admin or Policy Admin.

**Step 1** Choose Policy > Policy Elements > Conditions > Posture > Patch Management Condition.

**Step 2** Click Add.

**Step 3** Enter the condition name and description in the Name and Description fields.

**Step 4** Choose the appropriate operating system from the Operating System drop-down field.

**Step 5** Choose the Compliance Module from the drop-down list.

**Step 6** Choose the Vendor Name from the drop-down list.

**Step 7** Choose the Check Type.

**Step 8** Choose the appropriate patch from the Check patches installed drop-down list.

**Step 9** Click Submit.

**Related Topics**

- Patch Management Condition Settings, on page 1110
- Add a Patch Management Remediation, on page 793

Create Disk Encryption Conditions

You can create a policy to check if an end point is compliant with the specified data encryption software. For example, you can create a condition to check if the C: drive is encrypted in an end point. If the C: drive is not encrypted then the end point receives a non-compliance notification and ISE logs a message.

**Before you begin**

To perform the following task, you must be a Super Admin or Policy Admin. You can associate a Disk Encryption condition with a posture requirement only when you use the AnyConnect ISE posture agent.
Step 1  Choose Policy > Policy Elements > Conditions > Posture > Disk Encryption Condition.
Step 2  Click Add.
Step 3  In the Disk Encryption Condition page, enter the appropriate values in the fields.
Step 4  Click Submit.

Network Conditions

A policy is a set of conditions and a result. A policy condition consists of an operand (attribute), an operator (equal to, not equal to, greater than, and so on), and a value. Compound conditions are made up of one or more simple conditions that are connected by the AND or OR operator. At runtime, Cisco ISE evaluates a policy condition and then applies the result that you have defined based on whether the policy evaluation returns a true or a false value.

Each network condition defines a list of objects that can be included in policy conditions, resulting in a set of definitions that are matched against those presented in the request.

You can use the operator, EQUALS true, to check if the network condition evaluates to true (whether the value presented in the request matches at least one entry within the network condition) or EQUALS false to test whether the network condition evaluates to false (does not match any entry in the network condition).

After you create a network condition with a name, you can reuse this condition multiple times across various rules and policies by selecting the network condition from the Network Conditions dictionary, for example:

```
Network Conditions.MyNetworkCondition EQUALS true
```

You can create the following network conditions to restrict access to the network:

- Endstation Network Conditions—Based on endstations that initiate and terminate the connection.
  Cisco ISE evaluates the remote address TO field (which is obtained based on whether it is a TACACS+ or RADIUS request) to identify whether it is the IP address, MAC address, calling-line identification (CLI), or dialed number identification service (DNIS) of the endpoint.
  In a RADIUS request, this identifier is available in Attribute 31 (Calling-Station-Id).
  In a TACACS+ request, if the remote address includes a slash (/), the part before the slash is taken as the FROM value and the part after the slash is taken as the TO value. For example, if a request has CLI/DNIS, CLI is taken as the FROM value and DNIS is taken as the TO value. If a slash is not included, the entire remote address is taken as the FROM value (whether IP address, MAC address, or CLI).

- Device Network Conditions—Based on the AAA client that processes the request.
  A network device can be identified by its IP address, device name that is defined in the network device repository, or Network Device Group.
  In a RADIUS request, if Attribute 4 (NAS-IP-Address) is present, Cisco ISE obtains the IP address from this attribute. If Attribute 32 (NAS-Identifier) is present, Cisco ISE obtains the IP address from Attribute 32. If these attributes are not found, it obtains the IP address from the packet that it receives.
  The device dictionary (NDG dictionary) contains network device group attributes such as Location, Device Type, or other dynamically created attributes that represent NDGs. These attributes contain the groups that the current device is related to.
Configure Endstation Network Conditions

Step 1 Choose Policy > Policy Elements > Conditions > Network Conditions > Endstation Network Conditions.
Step 2 Click Add.
Step 3 Enter a name and description for the network condition.
Step 4 Enter the following details:
   • IP Addresses—You can add a list of IP addresses or subnets, one per line. The IP address/subnet can be in IPv4 or IPv6 format.
   • MAC Addresses—You can enter a list of Endstation MAC addresses and Destination MAC addresses, separated by a comma. Each MAC address must include 12 hexadecimal digits and must be in one of the following formats: nn:nn:nn:nn:nn:nn, nn-nn-nn-nn-nn-nn, nnnn.nnnn.nnnn, or nnnnnnnnnnnn. If the Endstation MAC or the Destination MAC is not required, use the token "-ANY-" instead.
   • CLI/DNIS—You can add a list of Caller IDs (CLI) and Called IDs (DNIS), separated by a comma. If the Caller ID (CLI) or the Called ID (DNIS) is not required, use the token "-ANY-" instead.
Step 5 Click Submit.

Configure Device Network Conditions

Step 1 Choose Policy > Policy Elements > Conditions > Network Conditions > Device Network Conditions.
Step 2 Click Add.
Step 3 Enter a name and description for the network condition.
Step 4 Enter the following details:
   • IP Addresses—You can add a list of IP addresses or subnets, one per line. The IP address/subnet can be in IPv4 or IPv6 format.
   • Device Name—You can add a list of device names, one per line. You must enter the same device name that is configured in the Network Device object.
   • Device Groups—You can add a list of tuples in the following order: Root NDG, comma, and an NDG (that it under the root NDG). There must be one tuple per line.
Configure Device Port Network Condition

Step 1 Choose Policy > Policy Elements > Conditions > Network Conditions > Device Port Network Conditions.
Step 2 Click Add.
Step 3 Enter a name and description for the network condition.
Step 4 Enter the following details:
   • IP Addresses—Enter the details in the following order: IP address or subnet, comma, and a port (that is used by the device). There must be one tuple per line.
   • Devices—Enter the details in the following order: device name, comma, and a port. There must be one tuple per line. You must enter the same device name that is configured in the Network Device object.
   • Device Groups—Enter the details in the following order: Root NDG, comma, NDG (that it under the root), and a port. There must be one tuple per line.

Step 5 Click Submit.

Create Time and Date Conditions

Use the Policy Elements Conditions page to display, create, modify, delete, duplicate, and search time and date policy element conditions. Policy elements are shared objects that define a condition that is based on specific time and date attribute settings that you configure.

Time and date conditions let you set or limit permission to access Cisco ISE system resources to specific times and days as directed by the attribute settings you make.

Before you begin
To perform the following task, you must be a Super Admin or Policy Admin.

Step 1 Choose Policy > Policy Elements > Conditions > Common > Time and Date > Add.
Step 2 Enter appropriate values in the fields.
   • In the Standard Settings area, specify the time and date to provide access.
   • In the Exceptions area, specify the time and date range to limit access.

Step 3 Click Submit.
CHAPTER 20

Manage Authentication Policies

- Cisco ISE Authentication Policies, on page 569
- Simple Authentication Policies, on page 572
- Rule-Based Authentication Policies, on page 574
- Policy Set Protocol Settings, on page 579
- Network Access Service, on page 584
- Network Access Work Center, on page 588
- Cisco ISE Acting as a RADIUS Proxy Server, on page 588
- Cisco ISE Acting as a TACACS+ Proxy Client, on page 590
- Location Based Authorization, on page 593
- Policy Modes, on page 595
- Configure a Simple Authentication Policy, on page 596
- Configure a Rule-Based Authentication Policy, on page 597
- Policy Sets, on page 598
- Authentication Policy Built-In Configurations, on page 601
- View Authentication Results, on page 604

Cisco ISE Authentication Policies

Authentication policies define the protocols that Cisco ISE uses to communicate with the network devices, and the identity sources that it uses for authentication. A policy is a set of conditions and a result. A policy condition consists of an operand (attribute), an operator (equal to, not equal to, greater than, and so on), and a value. Compound conditions are made up of one or more simple conditions that are connected by the AND or OR operator. At runtime, Cisco ISE evaluates a policy condition and then applies the result that you have defined based on whether the policy evaluation returns a true or a false value.

An authentication policy consists of the following:

- Network Access Service—This service can be one of the following:
  - An allowed protocols service to choose the protocols to handle the initial request and protocol negotiation.
  - A proxy service that will proxy requests to an external RADIUS server for processing.

- Identity Source—An identity source or an identity source sequence to be used for authentication.
After installation, a default identity authentication policy is available in Cisco ISE that is used for authentications. Any updates to the authentication policy will override the default settings.

**Related Topics**
- Policy Condition Evaluation, on page 570
- Supported Network Access Policy Set Protocols, on page 570
- Supported Authentication Types and Database, on page 570
- Authentication Failures—Policy Result Options, on page 571
- Authentication Policy Terminology, on page 572

**Policy Condition Evaluation**

During policy condition evaluation, Cisco ISE compares an attribute with a value. It is possible to run into a situation where the attribute specified in the policy condition may not have a value assigned in the request. In such cases, if the operator that is used for comparison is “not equal to,” then the condition will evaluate to true. In all other cases, the condition will evaluate to false.

For example, for a condition Radius.Calling_Station_IDNotEqualto 1.1.1.1, if the Calling Station ID is not present in the RADIUS request, then this condition will evaluate to true. This evaluation is not unique to the RADIUS dictionary and occurs because of the usage of the “Not Equal to” operator.

**Supported Network Access Policy Set Protocols**

The following is a list of protocols that you can choose while defining your Network Access Policy Set policy:

- Password Authentication Protocol (PAP)
- Protected Extensible Authentication Protocol (PEAP)
- Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2)
- Extensible Authentication Protocol-Message Digest 5 (EAP-MD5)
- Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)
- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST)
- Extensible Authentication Protocol-Tunneled Transport Layer Security (EAP-TTLS)
- Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)

**Related Topics**
- Supported Authentication Types and Database, on page 570
- Authentication Policy Terminology, on page 572
- Simple Authentication Policies, on page 572
- Rule-Based Authentication Policies, on page 574

**Supported Authentication Types and Database**

The authentication type is based on the protocols that are chosen. The authentication type is password based, where the authentication is performed against a database with the username and password that is presented in the request.
The identity method, which is the result of the authentication policy, can be any one of the following:

- Deny access—Access to the user is denied and no authentication is performed.
- Identity database—A single identity database that can be any one of the following:
  - Internal users
  - Guest users
  - Internal endpoints
  - Active Directory
  - Lightweight Directory Access Protocol (LDAP) database
  - RADIUS token server (RSA or SafeWord server)
  - Certificate authentication profile
- Identity source sequences—A sequence of identity databases that is used for authentication.

By default, the identity source that Cisco ISE will look up for user information is the internal users database.

**Authentication Failures—Policy Result Options**

If you choose the identity method as deny access, a reject message is sent as a response to the request. If you choose an identity database or an identity source sequence and the authentication succeeds, the processing continues to the authorization policy configured for the same policy set. Some of the authentications fail and these are classified as follows:

- Authentication failed—Received explicit response that authentication has failed such as bad credentials, disabled user, and so on. The default course of action is reject.
- User not found—No such user was found in any of the identity databases. The default course of action is reject.
- Process failed—Unable to access the identity database or databases. The default course of action is drop.

Cisco ISE allows you to configure any one of the following courses of action for authentication failures:

- Reject—A reject response is sent.
- Drop—No response is sent.
- Continue—Cisco ISE continues with the authorization policy.

Even when you choose the Continue option, there might be instances where Cisco ISE cannot continue processing the request due to restrictions on the protocol that is being used. For authentications using PEAP, LEAP, EAP-FAST, EAP-TLS, or RADIUS MSCHAP, it is not possible to continue processing the request when authentication fails or user is not found.

When authentication fails, it is possible to continue to process the authorization policy for PAP/ASCII and MAC authentication bypass (MAB or host lookup). For all other authentication protocols, when authentication fails, the following happens:

- Authentication failed—A reject response is sent.
• User or host not found—A reject response is sent.
• Process failure—No response is sent and the request is dropped.

Authentication Policy Terminology

The following are some of the commonly used terms in the authentication policy pages:

• Allowed Protocols—Allowed protocols define the set of protocols that Cisco ISE can use to communicate with the device that requests access to the network resources.

• Identity Source—Identity source defines which database Cisco ISE should use for user information. The database could be an internal database or an external identity source, such as Active Directory or LDAP. You can add a sequence of databases to an identity source sequence and list this sequence as the identity source in your policy. Cisco ISE will search for the credentials in the order in which the databases are listed in this sequence.

• Failover Options—You can define what course of action Cisco ISE should take if the authentication fails, the user is not found, or if the process fails.

Simple Authentication Policies

A simple authentication policy allows you to statically define the allowed protocols and the identity source or identity source sequence that Cisco ISE should use for communication. You cannot define any condition for simple policies. Cisco ISE assumes that all conditions are met and uses the following definitions to determine the result:

• You can create simple policies in situations where you can statically define the allowed protocols and the identity source that must be used always, and no condition needs to be checked.

• You can also create proxy service-based simple policies. Cisco ISE proxies the request to a policy server to determine which identity source should be used for user authentication. If the request is proxied to a different policy server, the protocol negotiation does not happen. The policy server evaluates which identity source should be used for authentication and returns the response to Cisco ISE.

Related Topics

Simple Authentication Policy Flow, on page 573
Guidelines for Configuring Simple Authentication Policies, on page 574
Define Allowed Protocols for Network Access, on page 584
Configure a Simple Authentication Policy, on page 596
Rule-Based Authentication Policies, on page 574
Simple Authentication Policy Flow

Figure 43: Simple Authentication Policy Flow

The result of a simple policy can be any one of the following:

- Authentication passed
- Authentication failed

An authentication can fail happens due to any of the following reasons:

- Bad credentials or disabled user.
- User not found.
- Authentication process fails.
Guidelines for Configuring Simple Authentication Policies

Follow these guidelines when configuring simple authentication policies:

- If you wish to use the RADIUS server sequence, then you must define this access service before you define the policy.
- If your users are defined in external identity sources, ensure that you have configured these identity sources in Cisco ISE before you define the policy.
- If you want to use an identity source sequence for authenticating users, ensure that you have created the identity source sequence before you define the policy.
- When you switch between simple and rule-based authentication policies, you will lose the policy that you configured earlier. For example, if you configured a simple authentication policy and you want to move to a rule-based authentication policy, you will lose the simple authentication policy. Also, when you move from a rule-based authentication policy to a simple authentication policy, you will lose the rule-based authentication policy.
- Host authentication is performed with the MAC address only (MAB).

Related Topics
Cisco ISE Acting as a RADIUS Proxy Server, on page 588

Rule-Based Authentication Policies

Rule-based authentication policies consist of attribute-based conditions that determine the allowed protocols and the identity source or identity source sequence to be used for processing the requests. In a simple authentication policy, you can define the allowed protocols and identity source statically. In a rule-based policy, you can define conditions that allows Cisco ISE to dynamically choose the allowed protocols and identity sources. You can define one or more conditions using any of the attributes from the Cisco ISE dictionary.

Cisco ISE allows you to create conditions as individual, reusable policy elements that can be referred from other rule-based policies. You can also create conditions from within the policy creation page. The two types of conditions are:
- Simple condition
- Compound condition

Related Topics
Attributes Supported by Dictionaries, on page 576
Configure a Rule-Based Authentication Policy, on page 597

Rule-Based Authentication Policy Flow

In rule-based policies, you can define multiple rules. The identity database is selected based on the first rule that matches the criteria.

You can also define an identity source sequence consisting of different databases. You can define the order in which you want Cisco ISE to look up these databases. Cisco ISE will access these databases in sequence.
until the authentication succeeds. If there are multiple instances of the same user in an external database, the authentication fails. There can only be one user record in an identity source.

We recommend that you use only three, or at most four databases in an identity source sequence.

**Figure 44: Rule-Based Authentication Policy Flow**

**Supported Dictionaries for Rule-Based Authentication Policies**

Cisco ISE supports the following dictionaries:

- System-defined dictionaries
  - CERTIFICATE
  - DEVICE
  - RADIUS
Attributes Supported by Dictionaries

The table lists the fixed attributes that are supported by dictionaries, which can be used in policy conditions. Not all of these attributes are available for creating all types of conditions.

For example, while creating a condition to choose the access service in authentication policies, you will only see the following network access attributes: Device IP Address, ISE Host Name, Network Device Name, Protocol, and Use Case.

You can use the attributes listed in the following table in policy conditions.

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Attributes</th>
<th>Allowed Protocol Rules and Proxy</th>
<th>Identity Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device</td>
<td>Device Type (predefined network device group)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Device Location (predefined network device group)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other Custom Network Device Group</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software Version</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Model Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RADIUS</td>
<td>All attributes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dictionary</td>
<td>Attributes</td>
<td>Allowed Protocol Rules and Proxy</td>
<td>Identity Rules</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------------------------------------</td>
<td>---------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Network Access</td>
<td>ISE Host Name</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>AuthenticationMethod</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>AuthenticationStatus</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>CTSDeviceID</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>Device IP Address</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>EapAuthentication (the EAP method that is used during authentication of a user of a machine)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>EapTunnel (the EAP method that is used for tunnel establishment)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Protocol</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>UseCase</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>UserName</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>WasMachineAuthenticated</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Dictionary</td>
<td>Attributes</td>
<td>Allowed Protocol Rules and Proxy</td>
<td>Identity Rules</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------</td>
<td>----------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Certificate</td>
<td>Common Name</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Country</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E-mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LocationSubject</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Organization</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Organization Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Serial Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>State or Province</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject Alternative Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject Alternative Name - DNS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject Alternative Name - E-mail</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject Alternative Name - Other Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject Serial Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Common Name</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Organization</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Organization Unit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Location</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Country</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Email</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Serial Number</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - State or Province</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Street Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - Domain Component</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Issuer - User ID</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Policy Set Protocol Settings

You must define global protocol settings in Cisco ISE before you can use these protocols to create, save and implement a policy set. You can use the Protocol Settings page to define global options for the Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), and Protected Extensible Authentication Protocol (PEAP) protocols, which communicate with the other devices in your network.

Related Topics
- Guidelines for Using EAP-FAST as Protocol, on page 579
- Configure EAP-FAST Settings, on page 580
- Generate the PAC for EAP-FAST, on page 580
- Configure EAP-TLS Settings, on page 581
- Configure PEAP Settings, on page 582
- Configure RADIUS Settings, on page 582

Guidelines for Using EAP-FAST as Protocol

Follow these guidelines when using EAP-FAST as an authentication protocol:

- It is highly recommended to enable EAP-TLS inner method when the EAP-FAST accept client certificate is enabled on authenticated provisioning. EAP-FAST accept client certificate on authenticated provisioning is not a separate authentication method but a shorter form of client certificate authentication that uses the same certificate credentials type to authenticate a user but does not require to run an inner method.

- Accept client certificate on authenticated provisioning works with PAC-less full handshake and authenticated PAC provisioning. It does not work for PAC-less session resume, anonymous PAC provisioning, and PAC-based authentication.

- EAP attributes are displayed per identity (so in EAP chaining displayed twice) are shown in authentication details in monitoring tool in order user then machine even if authentication happens in different order.

- When EAP-FAST authorization PAC is used then EAP authentication method shown in live logs is equal to the authentication method used for full authentication (as in PEAP) and not as Lookup.

- In EAP chaining mode when tunnel PAC is expired then ISE falls back to provisioning and AC requests User and Machine authorization PACs - Machine Authorization PAC cannot be provisioned. It will be provisioned in the subsequent PAC-based authentication conversation when AC requests it.

- When Cisco ISE is configured for chaining and AC for single mode then AC response with IdentityType TLV to ISE. However, the second identity authentication fails. You can see from this conversation that client is suitable to perform chaining but currently is configured for single mode.

- Cisco ISE supports retrieval attributes and groups for both machine and user in EAP-FAST chaining only for AD. For LDAP and Internal DB ISE uses only the last identity attributes.
“EAP-FAST cryptobinding verification failed” message might be seen if EAP-FAST authentication protocol is used for High Sierra MAC OSX devices. We recommend that you configure the Preferred EAP Protocol field in the Allowed Protocols page to use PEAP or EAP-TLS instead of EAP-FAST for High Sierra MAC OSX devices.

Configure EAP-FAST Settings

Before you begin
To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose Administration > System > Settings > Protocols > EAP-FAST > EAP Fast Settings.
Step 2 Enter the details as required to define the EAP-FAST protocol.
Step 3 Click Revoke if you want to revoke all the previously generated master keys and PACs.
Step 4 Click Save to save the EAP-FAST settings.

Related Topics
Generate the PAC for EAP-FAST, on page 580

Generate the PAC for EAP-FAST

You can use the Generate PAC option in the Cisco ISE to generate a tunnel or machine PAC for the EAP-FAST protocol.

Before you begin
To perform the following task, you must be a Super Admin or System Admin.

Step 1 Choose Administration > System > Settings.
Step 2 From the Settings navigation pane on the left, click Protocols.
Step 3 Choose EAP-FAST > Generate PAC.
Step 4 Enter the details as required to generate machine PAC for the EAP-FAST protocol.
Step 5 Click Generate PAC.

Using EAP-TTLS as Authentication Protocol

EAP-TTLS is a two-phase protocol that extends the functionality of EAP-TLS protocol. Phase 1 builds the secure tunnel and derives the session keys used in Phase 2 to securely tunnel attributes and inner method data between the server and the client. You can use the attributes tunneled during Phase 2 to perform additional authentications using a number of different mechanisms.
Cisco ISE can process authentications from a variety of TTLS supplicants including:

- AnyConnect Network Access Manager (NAM) on Windows
- Windows 8.1 native supplicant
- Secure W2 (also called as JoinNow on MultiOS)
- MAC OS X native supplicant
- IOS native supplicant
- Android based native supplicant
- Linux WPA supplicant

**Note**

If cryptobinding is required, you must use EAP-FAST as the inner method.

---

### Configure EAP-TTLS Settings

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

**Step 1** Choose Administration > System > Settings > Protocols > EAP-TTLS.

**Step 2** Enter the required details in the EAP-TTLS Settings page.

**Step 3** Click **Save**.

---

**Related Topics**

[ EAP-TTLS Settings, on page 956 ]

### Configure EAP-TLS Settings

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

**Step 1** Choose Administration > System > Settings > Protocols > EAP-TLS.

**Step 2** Enter the details as required to define the EAP-TLS protocol.

**Step 3** Click **Save** to save the EAP-TLS settings.
Configure PEAP Settings

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; System &gt; Settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the Settings navigation pane on the left, click Protocols.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose PEAP.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the details as required to define the PEAP protocol.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save to save the PEAP settings.</td>
</tr>
</tbody>
</table>

Configure RADIUS Settings

You can configure the RADIUS settings to detect the clients that fail to authenticate and to suppress the repeated reporting of successful authentications.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; System &gt; Settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the Settings navigation pane, click Protocols.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose RADIUS.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Enter the details as required to define the RADIUS settings.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Save to save the settings.</td>
</tr>
</tbody>
</table>

Configure Security Settings

To configure the security settings:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Administration &gt; System &gt; Settings &gt; Protocols &gt; Security Settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Security Settings page, select the required options:</td>
</tr>
</tbody>
</table>

- Allow TLS 1.0—Allows TLS 1.0 for communication with legacy peers for the following workflows:
  - Cisco ISE is configured as EAP server
  - Cisco ISE downloads CRL from HTTPS or secure LDAP server
  - Cisco ISE is configured as secure syslog client
  - Cisco ISE is configured as secure LDAP client

- Allow TLS 1.1—Allows TLS 1.1 for communication with legacy peers for the following workflows:
  - Cisco ISE is configured as EAP server
• Cisco ISE downloads CRL from HTTPS or secure LDAP server
• Cisco ISE is configured as secure syslog client
• Cisco ISE is configured as secure LDAP client

• Allow SHA1 Ciphers—Allows SHA-1 ciphers for communication with peers for the following workflows:
  • Cisco ISE is configured as EAP server
  • Cisco ISE is configured as RADIUS DTLS server
  • Cisco ISE is configured as RADIUS DTLS client
  • Cisco ISE downloads CRL from HTTPS or secure LDAP server
  • Cisco ISE is configured as secure syslog client
  • Cisco ISE is configured as secure LDAP client

Note: It is recommended to use SHA-256 or SHA-384 ciphers for enhanced security.

• Allow ECDHE-RSA Ciphers—Allow ECDHE-RSA ciphers for communication with peers for the following workflows:
  • Cisco ISE is configured as EAP server
  • Cisco ISE is configured as RADIUS DTLS server
  • Cisco ISE is configured as RADIUS DTLS client
  • Cisco ISE downloads CRL from HTTPS or secure LDAP server
  • Cisco ISE is configured as secure syslog client
  • Cisco ISE is configured as secure LDAP client

• Allow 3DES ciphers—Allow 3DES ciphers for communication with peers for the following workflows:
  • Cisco ISE is configured as EAP server
  • Cisco ISE is configured as RADIUS DTLS server
  • Cisco ISE is configured as RADIUS DTLS client
  • Cisco ISE downloads CRL from HTTPS or secure LDAP server
  • Cisco ISE is configured as secure syslog client
  • Cisco ISE is configured as secure LDAP client

• Accept Certificates without Validating Purpose—When ISE acts as an EAP or RADIUS DTLS server, client certificates are accepted without checking whether the Key Usage extension contains keyAgreement bit for ECDHE-ECDSA ciphers or keyEncipherment bit for other ciphers.

• Allow DSS ciphers for ISE as a client—When Cisco ISE acts as a client, allow DSS ciphers for communication with server for the following workflows:
  • Cisco ISE is configured as RADIUS DTLS client
- Cisco ISE downloads CRL from HTTPS or secure LDAP server
- Cisco ISE is configured as secure syslog client
- Cisco ISE is configured as secure LDAP client

- Allow Legacy Unsafe TLS Renegotiation for ISE as a Client—Allows communication with legacy TLS servers that do not support safe TLS renegotiation for the following workflows:
  - Cisco ISE downloads CRL from HTTPS or secure LDAP server
  - Cisco ISE is configured as secure syslog client
  - Cisco ISE is configured as secure LDAP client

---

**Network Access Service**

A network access service contains the authentication policy conditions for requests. You can create separate network access services for different use cases, for example, Wired 802.1X, Wired MAB, and so on. To create a network access service, configure allowed protocols or server sequences. The network access service for network access policies is then configured from the Policy Sets page.

**Related Topics**
- Define Allowed Protocols for Network Access, on page 584
- Cisco ISE Acting as a RADIUS Proxy Server, on page 588
- Simple Authentication Policies, on page 572
- Configure a Rule-Based Authentication Policy, on page 597

**Define Allowed Protocols for Network Access**

Allowed protocols define the set of protocols that Cisco ISE can use to communicate with the device that requests access to the network resources. An allowed protocols access service is an independent entity that you should create before you configure authentication policies. Allowed protocols access service is an object that contains your chosen protocols for a particular use case.

The Allowed Protocols Services page lists all the allowed protocols services that you create. There is a default network access service that is predefined in the Cisco ISE.

**Before you begin**

Before you begin this procedure, you should have a basic understanding of the protocol services that are used for authentication.

- Review the Cisco ISE Authentication Policies section in this chapter to understand authentication type and the protocols that are supported by various databases.
• Review the PAC Options to understand the functions and options for each protocol service, so you can make the selections that are appropriate for your network.

• Ensure that you have defined the global protocol settings.

To perform the following task, you must be a Super Admin or System Admin.

**Step 1** Choose Policy > Policy Elements > Results > Authentication > Allowed Protocols.
If Cisco ISE is set to operate in FIPS mode, some protocols are disabled by default and cannot be configured.

**Step 2** Click Add.

**Step 3** Enter the required information.

**Step 4** Select the appropriate authentication protocols and options for your network.

**Step 5** If you choose to use PACs, make the appropriate selections.
To enable Anonymous PAC Provisioning, you must choose both the inner methods, EAP-MSCHAPv2 and Extensible Authentication Protocol-Generic Token Card (EAP-GTC). Also, be aware that Cisco ISE only supports Active Directory as an external identity source for machine authentication.

**Step 6** Click Submit to save the allowed protocols service.
The allowed protocols service appears as an independent object in the simple and rule-based authentication policy pages. You can use this object in different rules.

You can now create a simple or rule-based authentication policy.
If you disable EAP-MSCHAP as inner method and enable EAP-GTC and EAP-TLS inner methods for PEAP or EAP-FAST, ISE starts EAP-GTC inner method during inner method negotiation. Before the first EAP-GTC message is sent to the client, ISE executes identity selection policy to obtain GTC password from the identity store. During the execution of this policy, EAP authentication is equal to EAP-GTC. If EAP-GTC inner method is rejected by the client and EAP-TLS is negotiated, identity store policy is not executed again. In case identity store policy is based on EAP authentication attribute, it might have unexpected results since the real EAP authentication is EAP-TLS but was set after identity policy evaluation.

**Related Topics**
Cisco ISE Authentication Policies, on page 569
Policy Set Protocol Settings, on page 579

**Enable MAB from Non-Cisco Devices**
Configure the following settings sequentially to configure MAB from non-Cisco devices.

**Step 1** Ensure that the MAC address of the endpoints that are to be authenticated are available in the Endpoints database. You can add these endpoints or have them profiled automatically by the Profiler service.

**Step 2** Create a Network Device Profile based on the type of MAC authentication used by the non-Cisco device (PAP, CHAP, or EAP-MD5).
   a) Choose Administration > Network Resources > Network Device Profiles.
   b) Click Add.
c) Enter a name and description for the network device profile.
d) Select the vendor name from the Vendor drop-down list.
e) Check the check boxes for the protocols that the device supports. If the device supports RADIUS, select the RADIUS
dictionary to use with the network device.
f) Expand the Authentication/Authorization section to configure the device's default settings for flow types, attribute
aliasing, and host lookup.
g) In the Host Lookup (MAB) section, do the following:

   • Process Host Lookup—Check this check box to define the protocols for host lookup used by the network device
      profile.
   
   Network devices from different vendors perform MAB authentication differently. Depending on the device type,
   check the Check Password check box and/or Check Calling-Station-Id equals MAC Address check box, for
   the protocol you are using.
   
   • Via PAP/ASCII—Check this check box to configure Cisco ISE to detect a PAP request from the network device
      profile as a Host Lookup request.
   
   • Via CHAP—Check this check box to configure Cisco ISE to detect this type of request from the network devices
      as a Host Lookup request.
   
   • Via EAP-MD5—Check this check box to enable EAP-based MD5 hashed authentication for the network device
      profile.

h) Enter the required details in the Permissions, Change of Authorization (CoA), and Redirect sections, and then click
Submit.

For information on how to create custom NAD profiles, see Network Access Device Profiles with Cisco Identity
Services Engine.

**Step 3** Choose Administration > Network Resources > Network Devices.

**Step 4** Select the device for which you want to enable MAB, and then click Edit.

**Step 5** In the Network Device page, select the network device profile that you created in step 2 from the Device Profile drop-down
list.

**Step 6** Click Save.

---

**Note**

For Cisco NADs, the Service-Type values used for MAB and web/user authentication are different. This
allows ISE to differentiate MAB from web authentication when Cisco NADs are used. Some non-Cisco NADs
use the same value for the Service-Type attribute for both MAB and web/user authentication; this may lead
to security issues in your access policies. If you are using MAB with non-Cisco devices, we recommend that
you configure additional authorization policy rules to ensure that your network security is not compromised.
For example, if a printer is using MAB, you could configure an authorization policy rule to restrict it to printer
protocol ports in the ACL.

**Related Topics**

Define Allowed Protocols for Network Access, on page 584

Configure a Rule-Based Authentication Policy, on page 597
Enable MAB from Cisco Devices

Configure the following settings sequentially to configure MAB from Cisco devices.

**Step 1**
Ensure that the MAC address of the endpoints that are to be authenticated are available in the Endpoints database. You can add these endpoints or have them profiled automatically by the Profiler service.

**Step 2**
Create a Network Device Profile based on the type of MAC authentication used by the Cisco device (PAP, CHAP, or EAP-MD5).

a) Choose Administration > Network Resources > Network Device Profiles.
b) Click Add.
c) Enter a name and description for the network device profile.
d) Check the check boxes for the protocols that the device supports. If the device supports RADIUS, select the RADIUS dictionary to use with the network device.
e) Expand the Authentication/Authorization section to configure the device's default settings for flow types, attribute aliasing, and host lookup.
f) In the Host Lookup (MAB) section, do the following:
   • Process Host Lookup—Check this check box to define the protocols for host lookup used by the network device profile.
     Depending on the device type, check the Check Password check box and/or Check Calling-Station-Id equals MAC Address check box, for the protocol you are using.
   • Via PAP/ASCII—Check this check box to configure Cisco ISE to detect a PAP request from the network device profile as a Host Lookup request.
   • Via CHAP—Check this check box to configure Cisco ISE to detect this type of request from the network devices as a Host Lookup request.
   • Via EAP-MD5—Check this check box to enable EAP-based MD5 hashed authentication for the network device profile.

g) Enter the required details in the Permissions, Change of Authorization (CoA), and Redirect sections, and then click Submit.

For information on how to create custom NAD profiles, see Network Access Device Profiles with Cisco Identity Services Engine.

**Step 3**
Choose Administration > Network Resources > Network Devices.

**Step 4**
Select the device for which you want to enable MAB, and then click Edit.

**Step 5**
In the Network Device page, select the network device profile that you created in step 2 from the Device Profile drop-down list.

**Step 6**
Click Save.

ISE Community Resource
For information about IP phone authentication capabilities, see Phone Authentication Capabilities.

Related Topics
Define Allowed Protocols for Network Access, on page 584
Network Access Work Center

Network Access related options are grouped under the Network Access Work Center menu (Work Centers > Network Access), so that the administrator can easily access all the options related to Network Access at one location.

You can perform the following tasks from the Network Access Work Center:

• Configure the external identity stores that you intend to use during the authentication process for users and devices. You can configure the following external identity stores: Active Directory, LDAP, ODBC, RADIUS, RSA, and SAML ID Providers.

• Define policy elements to be used in the authentication and authorization policies.

• Add all the network devices that will be controlled by Cisco ISE. Devices can be grouped by type and location.

• Define authentication and authorization policies for users and network devices based on your requirements.

• Check default network access settings for client provisioning, protocol settings, and proxy configuration.

• Monitor network events by using RADIUS Livelog.

• Run network access reports to check access and authorization results.

• Troubleshoot network access issues using the diagnostic tools.

Cisco ISE Acting as a RADIUS Proxy Server

Cisco ISE can function both as a RADIUS server and as a RADIUS proxy server. When it acts as a proxy server, Cisco ISE receives authentication and accounting requests from the network access server (NAS) and forwards them to the external RADIUS server. Cisco ISE accepts the results of the requests and returns them to the NAS.

Cisco ISE can simultaneously act as a proxy server to multiple external RADIUS servers. You can use the external RADIUS servers that you configure here in RADIUS server sequences. The External RADIUS Server page lists all the external RADIUS servers that you have defined in Cisco ISE. You can use the filter option to search for specific RADIUS servers based on the name or description, or both. In both simple and rule-based authentication policies, you can use the RADIUS server sequences to proxy the requests to a RADIUS server.

The RADIUS server sequence strips the domain name from the RADIUS-Username attribute for RADIUS authentications. This domain stripping is not applicable for EAP authentications, which use the EAP-Identity attribute. The RADIUS proxy server obtains the username from the RADIUS-Username attribute and strips it from the character that you specify when you configure the RADIUS server sequence. For EAP authentications, the RADIUS proxy server obtains the username from the EAP-Identity attribute. EAP authentications that use the RADIUS server sequence will succeed only if the EAP-Identity and RADIUS-Username values are the same.
Configure External RADIUS Servers

You must configure the external RADIUS servers in the Cisco ISE to enable it to forward requests to the external RADIUS servers. You can define the timeout period and the number of connection attempts.

Before you begin

- You cannot use the external RADIUS servers that you create in this section by themselves. You must create a RADIUS server sequence and configure it to use the RADIUS server that you create in this section. You can then use the RADIUS server sequence in authentication policies.
- To perform the following task, you must be a Super Admin or System Admin.

**Step 1** Choose Administration > Network Resources > External RADIUS Servers.

The RADIUS Servers page appears with a list of external RADIUS servers that are defined in Cisco ISE.

**Step 2** Click Add to add an external RADIUS server.

**Step 3** Enter the values as required.

**Step 4** Click Submit to save the external RADIUS server configuration.

**Related Topics**

- RADIUS Server Sequence

Define RADIUS Server Sequences

RADIUS server sequences in Cisco ISE allow you to proxy requests from a NAD to an external RADIUS server that will process the request and return the result to Cisco ISE, which forwards the response to the NAD.

RADIUS Server Sequences page lists all the RADIUS server sequences that you have defined in Cisco ISE. You can create, edit, or duplicate RADIUS server sequences from this page.

Before you begin

- Before you begin this procedure, you should have a basic understanding of the Proxy Service and must have successfully completed the task in the first entry of the Related Links.
- To perform the following task, you must be a Super Admin or System Admin.

**Step 1** Choose Administration > Network Resources > RADIUS Server Sequences.

**Step 2** Click Add.

**Step 3** Enter the values as required.

**Step 4** Click Submit to save the RADIUS server sequence to be used in policies.

**Related Topics**

- Configure External RADIUS Servers, on page 589
Cisco ISE Acting as a TACACS+ Proxy Client

Cisco ISE can act as proxy client to external TACACS+ servers. When it acts as a proxy client, Cisco ISE receives authentication, authorization, and accounting requests from the Network Access Server (NAS) and forwards them to the external TACACS+ server. Cisco ISE accepts the results of the requests and returns them to the NAS.

The TACACS+ External Servers page lists all the external TACACS+ servers that you have defined in Cisco ISE. You can use the filter option to search for specific TACACS+ servers based on the name or description, or both.

Cisco ISE can simultaneously act as a proxy client to multiple external TACACS+ servers. In order to configure multiple external servers, you can use the TACACS+ server sequence page. Refer to the TACACS+ Server Sequence Settings page for more information.

Related Topics
- TACACS+ External Server Settings, on page 590
- Configure External TACACS+ Servers, on page 591
- TACACS+ Server Sequence Settings, on page 592
- Define TACACS+ Server Sequences, on page 593

TACACS+ External Server Settings

The following table describes the fields in the TACACS External Servers page. The navigation path is Work Centers > Device Administration > Network Resources > TACACS External Servers page.

Table 38: TACACS+ External Server Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the TACACS+ external server.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the TACACS+ external server setting.</td>
</tr>
<tr>
<td>Host IP</td>
<td>Enter the IP address (IPv4 or IPv6 address) of the remote TACACS+ external server.</td>
</tr>
<tr>
<td>Connection Port</td>
<td>Enter the port number of the remote TACACS+ external server. The port number is 49.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Specify the number of seconds that ISE should wait for a response from the external TACACS+ server. The default is 5 seconds. Valid values are from 1 to 120.</td>
</tr>
</tbody>
</table>
### Configure External TACACS+ Servers

You must configure the external TACACS servers in the Cisco ISE to enable it to forward requests to the external TACACS servers. You can define the timeout period and the number of connection attempts.

**Before you begin**

- You cannot use the external TACACS servers that you create in this section directly in the policy. You must create a TACACS server sequence and configure it to use the TACACS server that you create in this section. You can then use the TACACS server sequence in the policy sets.
- To perform the following task, you must be a Super Admin or System Admin.

<table>
<thead>
<tr>
<th>Step</th>
<th>Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose <strong>Work Centers &gt; Device Administration &gt; Network Resources &gt; TACACS External Servers</strong>. The <strong>TACACS External Servers</strong> page appears with a list of external TACACS servers that are defined in Cisco ISE.</td>
</tr>
<tr>
<td>2</td>
<td>Click <strong>Add</strong> to add an external TACACS server.</td>
</tr>
<tr>
<td>3</td>
<td>Enter the values as required.</td>
</tr>
<tr>
<td>4</td>
<td>Click <strong>Submit</strong> to save the external TACACS server configuration.</td>
</tr>
</tbody>
</table>

**Related Topics**

- [TACACS+ External Server Settings](#), on page 590
- [Configure External TACACS+ Servers](#), on page 591
- [TACACS+ Server Sequence Settings](#), on page 592
- [Define TACACS+ Server Sequences](#), on page 593
TACACS+ Server Sequence Settings

The following table describes the fields in the TACACS Server Sequence page. The navigation path is **Work Centers > Device Administration > Network Resources > TACACS Server Sequence** page.

**Table 39: TACACS+ Server Sequence Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the TACACS proxy server sequence.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the TACACS proxy server sequence.</td>
</tr>
<tr>
<td>Server List</td>
<td>Select the required TACACS proxy servers from the Available list. The available list contains the list of TACACS proxy servers configured in the TACACS External Services Page.</td>
</tr>
<tr>
<td>Logging Control</td>
<td>Check to enable logging control:</td>
</tr>
<tr>
<td></td>
<td>• Local Accounting: Accounting messages are logged by the server that handles requests from devices.</td>
</tr>
<tr>
<td></td>
<td>• Remote Accounting: Accounting messages are logged by the proxy server that handles requests from devices.</td>
</tr>
<tr>
<td>Username Stripping</td>
<td>Username Prefix/Suffix Stripping:</td>
</tr>
<tr>
<td></td>
<td>• Prefix Strip: Check to strip the username from the prefix. For example, if the subject name is <code>acme\smith</code> and the separator is <code>\</code>, the username becomes smith. The default separator is <code>\</code>.</td>
</tr>
<tr>
<td></td>
<td>• Suffix Strip: Check to strip the username from the suffix. For example, if the subject name is <code>smith@acme.com</code> and the separator is <code>@</code>, the username becomes smith. The default separator is <code>@</code>.</td>
</tr>
</tbody>
</table>

**Related Topics**

- [TACACS+ External Server Settings](#), on page 590
- [Configure External TACACS+ Servers](#), on page 591
- [TACACS+ Server Sequence Settings](#), on page 592
- [Define TACACS+ Server Sequences](#), on page 593
Define TACACS+ Server Sequences

TACACS+ server sequences in Cisco ISE allow you to proxy requests from a NAD to an external TACACS+ server that will process the request and return the result to Cisco ISE, which forwards the response to the NAD. The TACACS+ Server Sequences page lists all the TACACS+ server sequences that you have defined in Cisco ISE. You can create, edit, or duplicate TACACS+ server sequences from this page.

Before you begin

- You should have a basic understanding of the Proxy Service, Cisco ISE Admin Groups, Access Levels, Permissions, and Restrictions.
- To perform the following task, you must be a Super Admin or System Admin.
- Ensure that the external TACACS+ servers that you intend to use in the TACACS+ server sequence are already defined.

Step 1 Choose Work Centers > Device Administration > Network Resources > TACACS External Server Sequence.
Step 2 Click Add.
Step 3 Enter the required values.
Step 4 Click Submit to save the TACACS+ server sequence to be used in policies.

Related Topics

- TACACS+ External Server Settings, on page 590
- Configure External TACACS+ Servers, on page 591
- TACACS+ Server Sequence Settings, on page 592
- Define TACACS+ Server Sequences, on page 593

Location Based Authorization

Cisco ISE integrates with Cisco Mobility Services Engine (MSE) to introduce physical location-based authorization. Cisco ISE uses information from MSE to provide differentiated network access based on the actual location of the user, as reported by MSE.

With this feature, you can use the endpoint location information to provide network access when a user is in an appropriate zone. You can also add the endpoint location as an additional attribute for policies to define more granulated policy authorization sets based on device location. You can configure conditions within authorization rules that use location-based attributes, for example:

MSE.Location equals LND_Campus1:Building1:Floor2:SecureZone

You can define the location hierarchy (campus/building/floor structure) and configure the secure and non-secure zones using the Cisco Prime Infrastructure application. After defining the location hierarchy, you must synchronize the location hierarchy data with the MSE servers. For more information on Cisco Prime Infrastructure, see: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-infrastructure/products-user-guide-list.html.
You can add one or multiple MSE instances to integrate MSE-based location data to the authorization process. You can retrieve the location hierarchy data from these MSEs and configure location-based authorization rules using this data.

To track the endpoint movement, check the Track Movement check box while creating an authorization profile. Cisco ISE will query the relevant MSE for the endpoint location every 5 minutes to verify if the location was changed.

---

**Note**
Tracking multiple users will impact the performance due to frequent updates. The Track Movement option can be used for high security locations.

The Location Tree is created by using the location data retrieved from the MSE instances. You can select the location entries that are exposed to the authorization policy by using the Location Tree.

---

**Note**
You will need ISE Plus license to use the Location Services.

### Add a MSE server

#### Before you begin
To perform the following task, you must be a Super Admin or System Admin.

---

**Step 1**
Choose *Administration > Network Resources > Location Services > Location Servers.*

**Step 2**
Click *Add.*

**Step 3**
Enter the MSE server details, such as server name, hostname/IP address, password, and so on.

**Step 4**
Click *Test* to test MSE connectivity using the server details that you have provided.

**Step 5**
(Optional) Enter the MAC address of an endpoint in the **Find Location** field and click **Find** to check whether the endpoint is currently connected to this MSE.

If the endpoint location is found, it is displayed in the following format: *Campus:Building:Floor:Zone.* Sometimes, more than one entry can be displayed depending on the location hierarchy and zone settings. For example, if all the floors of a building (*building1*) in a campus named *Campus1* are defined as non-secure zones, and the Lab Area in the first floor is defined as a secure zone, the following entries will be displayed when the endpoint is located in the Lab Area:

Found in:

`Campus1#building1#floor1#LabArea`

`Campus1#building1#floor1#NonSecureZone`

**Step 6**
Click *Submit.*

After a new MSE is added, go to the Location Tree page and click **Get Update** to retrieve its location hierarchy and add it to the Location Tree. If there are filters defined on this tree, these filters are applied on the new MSE entries as well.
Location Tree

The Location Tree is created by using the location data retrieved from the MSE instances. To view the Location Tree, choose Administration > Network Resources > Location Services > Location Tree.

If one building has multiple MSEs, Cisco ISE will collate the location details from all the MSEs and present them as a single tree.

You can select the location entries that are exposed to the authorization policy by using the Location Tree. You can also hide specific locations based on your requirements. It is recommended to update the Location Tree before hiding locations. Hidden locations will remain hidden even when the tree is updated.

If the location entries related to an authorization rule are modified or removed, you must disable the affected rules and set these locations as Unknown or select a replacement location for each affected rule. You must verify the new tree structure before applying the change or canceling the update.

Click Get Update to get the latest location hierarchy structure from all MSEs. After verifying the new tree structure, click Save to apply your changes.

Policy Modes

Cisco ISE provides two types of policy modes, the Simple mode and the Policy Set mode. You can select either one of these to configure authentication and authorization policies. When you change the policy mode, you are prompted to login again to the Cisco ISE interface. If you switch from the Policy Set mode to the Simple mode, all the policy set data is deleted except the default policy. The Policy menu options change based on the policy mode selection.

- Simple Mode—If you select Simple mode, you can define authentication and authorization policies separately in the Policy menu.

  Figure 45: Simple Mode Policy Menu

- Policy Set Mode—If you select Policy Set mode, you can create policy sets and logically group authentication and authorization within the same group. You can have several groups based on what you need.

  Figure 46: Policy Set Mode Policy Menu
Change Policy Modes

The following are the guidelines for changing policy modes:

• After you do a fresh install or upgrade from Cisco ISE, Release 1.1, the Simple Mode policy model is selected by default.

• If you choose to switch to Policy Set Mode from Simple Mode, the authentication and authorization policies are migrated to the default policy set.

• If you choose to switch to Simple Mode from Policy Set Mode, the authentication and authorization of the default policy set are migrated to be the authentication and authorization policies. All other policy set policies are deleted.

Step 1  Choose Administration > System > Settings > Policy Sets.
Step 2  Enable or Disable the Policy Set mode.
Step 3  Click Save.

You will be prompted to login again, for the new policy mode to come into effect.

Configure a Simple Authentication Policy

The procedure for configuring a simple authentication policy includes defining an allowed protocols service and configuring a simple authentication policy.

Before you begin

• To configure a simple authentication policy using the RADIUS server sequence, you should have a basic understanding of the Cisco ISE authentication policies and proxy service to understand authentication types and the protocols that are supported by various databases.

• You should have defined an allowed protocol access service or RADIUS server sequence.

• To perform the following task, you must be a Super Admin or System Admin.

You can also use this process to configure a simple policy using RADIUS server sequence.
Configure a Rule-Based Authentication Policy

In a rule-based policy, you can define conditions that allows Cisco ISE to dynamically choose the allowed protocols and identity sources. You can define one or more conditions using any of the attributes from the Cisco ISE dictionary.

**Tip**

We recommend that you create the allowed protocol access services, conditions, and identity source sequences before you create the rule-based authentication policy. If you want to use the RADIUS server sequence, you can define the RADIUS server sequence before you create the policy.

**Before you begin**

- You should have a basic understanding of the rule-based authentication policies, defined allowed protocols for network access, created identity source sequence, and RADIUS server sequence (if you want to use the RADIUS server sequence in place of the allowed protocol access service).

- Cisco ISE comes with predefined rule-based authentication policies for the Wired 802.1X, Wireless 802.1X, and Wired MAB use cases.

- To perform the following task, you must be a Super Admin or System Admin.

- If your users are defined in external identity sources, ensure that you have configured these identity sources in Cisco ISE.

**Note**

When you switch between a simple and a rule-based authentication policy, you will lose the policy that you configured earlier. For example, if you have a simple authentication policy configured and you want to move to a rule-based authentication policy, you will lose the simple authentication policy. Also, when you move from a rule-based authentication policy to a simple authentication policy, you will lose the rule-based authentication policy.
Step 1  Choose Policy > Authentication.

Step 2  Click the Rule-Based radio button.

Step 3  Click OK on the message that appears.

Step 4  Click the action icon and click Insert new row above or Insert new row below based on where you want the new policy to appear in this list. The policies will be evaluated sequentially.

Each row in this rule-based policy page is equivalent to the simple authentication policy. Each row contains a set of conditions that determine the allowed protocols and identity sources.

Step 5  Enter the values as required to create a new authentication policy.

Step 6  Click Save to save your rule-based authentication policies.

You cannot specify the “UserName” attribute when configuring an authentication policy when the EAP-FAST client certificate is sent in the outer TLS negotiation. Cisco recommends using certificate fields like “CN” and “SAN,” for example.

ISE does not restrict a user or machine EAP-TLS authentication against Active Directory when the account in Active Directory is set to deny the user or machine using logon hours, locked-out, or workstations attributes. You should not use these attributes to restrict a user or machine for EAP-TLS authentications.

**Related Topics**

- Rule-Based Authentication Policies, on page 574
- Configure a Rule-Based Authentication Policy, on page 597
- Define Allowed Protocols for Network Access, on page 584
- RADIUS Server Sequence Authentication Policy Built-In Configurations, on page 601
- Attributes Supported by Dictionaries, on page 576
- Cisco ISE Acting as a RADIUS Proxy Server, on page 588
- Cisco ISE Authentication Policies, on page 569

**Default Authentication Policy**

The last row in the authentications policy page is the default policy that will be applied if none of the rules match the request. You can edit the allowed protocols and identity source selection for the default policy.

It is a good practice to choose Deny Access as the identity source in the default policy if the request does not match any of the other policies that you have defined.

**Policy Sets**

Policy sets enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type and similar parameters.

Policy sets are first-match policies. Each policy has a condition that can be a simple or a compound condition, and have the following supported dictionaries:

- Airspace
Once the policy set is matched and selected, its authentication and authorization policies are evaluated. In addition, a global authorization exception policy is available as part of the policy set model.

There is always one policy set defined, which is the default policy set.

Related Topics
- Policy Set Evaluation Flow, on page 599
- Configure Policy Sets, on page 600
- Global Authorization Exception Policy, on page 600
- Configure Policy Sets, on page 601

### Policy Set Evaluation Flow

**Figure 47: Policy Set Authentication and Authorization Evaluation Flow**

The sequence of policy set and the authentication and authorization evaluation flow is as follows:

1. Evaluate policy set (by evaluating the policy set condition). As a result, one policy set is selected.
2. Evaluate allowed protocols rules of the selected policy set.
3. Evaluate ID store rules of the selected policy set.
4. Evaluate authorization rules of the selected policy set, based on the following paradigm:
   - Evaluate the local exception policy in case it is defined
   - If no match is found in Step 1 above, evaluate global exception policy if defined
   - If no match is found in Step 2 above, evaluate authorization rules
   - If none of the policy set matches, the default policy set will be selected.

Configure Policy Sets

Configure policy sets in order to manage your authentication and authorization policy flows.

Following are the guidelines for creating policy sets:

• Rules are configured with names, conditions, and results. You must define authentication and authorization rules in order to implement a policy set. The default pre-configured policy set that is installed automatically with ISE, as well as any new policy sets that you create, are automatically created with the existing default authentication and authorization policy rules which you can then edit or supplement.

• Conditions may be stored in the Library of the Conditions Studio and can be used for multiple policy sets thereafter.

Overview of Steps for Configuring a Policy Set

Following are the steps for configuring a complete policy set including authentication, exception and authorization rules:

1. Upon installing ISE, a default policy set is implemented, including default ISE authentication and authorization rules. The default policy set also includes additional flexible built-in rules (that are not defaults) for authentication and authorization. You can add additional rules to those policies and you can delete and change the built-in rules but you cannot remove the default rules and you cannot remove the default policy set.
   - If you want to customize your sets and rules, you can first create your own conditions, identity sources, security groups and authorization profiles. Alternatively, you can configure your customizations while working with the policy sets that you are creating. For example, while adding rules to your authorization policy, you can select Create a New Authorization Profile in order to customize an authorization profile and to add it to the policy set that you are currently editing.

2. Create policy sets.

3. Configure authentication policies.

4. Configure authorization policies.

Global Authorization Exception Policy

The global authorization exception policy allows you to define rules that apply to all policy sets. The global authorization exception policy is added to each authorization policy of all the policy set. Global authorization exception policy can be updated by selecting the Global Exceptions option from the policy set list.

Each authorization policy can have local exception rule, global exception rule, and regular rules. Once you configure the local authorization exception rule, (for some authorization policies) the global exception
Authorization rules are displayed in read-only mode in conjunction to the local authorization exception rule. The local authorization exception rule can overwrite the global exception rule. The authorization rules are processed in the following order: first the local exception rule, then the global exception rule, and finally, the regular rule of the authorization policy.

### Configure Policy Sets

You can use this page to configure Policy sets.

**Before you begin**

You should have selected the policy mode as Policy Set to be able to configure Policy sets. To do this, go to Administration > System > Settings > Policy Sets.

1. **Step 1** Choose Policy > Policy Sets.
2. **Step 2** Click the Default policy. The default policy is displayed in the right.
3. **Step 3** Click the plus (+) sign on top and choose Create Above.
4. **Step 4** Enter the name, description and a condition for this group policy.
5. **Step 5** Define the authentication policy.
6. **Step 6** Define the authorization policy.
7. **Step 7** Click Submit. After you configure a policy set, Cisco ISE logs you out. You must log in again to access the Admin portal.

**Related Topics**

- Change Policy Modes, on page 596
- Configure a Rule-Based Authentication Policy, on page 597
- Policy Set Evaluation Flow, on page 599
- Configure Policy Sets, on page 600
- Global Authorization Exception Policy, on page 600

### Authentication Policy Built-In Configurations

Cisco ISE is packaged with several default configurations that are part of common use cases.

**Table 40: Authentication Policy Configuration Defaults**

<table>
<thead>
<tr>
<th>Name</th>
<th>Path in the User Interface</th>
<th>Description</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Network Access Allowed Protocols Access Service</td>
<td>Policy &gt; Policy Elements &gt; Configuration &gt; Allowed Protocols</td>
<td>This default is the built-in network access allowed protocols service to be used in authentication policies.</td>
<td>You can use this access service for wired and wireless 802.1X, and wired MAB authentication policies.</td>
</tr>
<tr>
<td>Name</td>
<td>Path in the User Interface</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Wired 802.1X Compound Condition</td>
<td>Policy &gt; Policy Elements &gt; Conditions &gt; Authentication &gt;</td>
<td>This compound condition checks for the following attributes and values:</td>
<td>This compound condition is used in the wired 802.1X authentication policy. Any request that matches the criteria specified in this policy would be evaluated based on the wired 802.1X authentication policy.</td>
</tr>
<tr>
<td></td>
<td>Compound Conditions</td>
<td>• RADIUS:Service-Type equals Framed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RADIUS:NAS-Port-Type equals Ethernet</td>
<td></td>
</tr>
<tr>
<td>Wireless 802.1X Compound Condition</td>
<td>Policy &gt; Policy Elements &gt; Conditions &gt; Authentication &gt;</td>
<td>This compound condition checks for the following attributes and values:</td>
<td>This compound condition is used in the wireless 802.1X authentication policy. Any request that matches the criteria specified in this policy would be evaluated based on the wireless 802.1X authentication policy.</td>
</tr>
<tr>
<td></td>
<td>Compound Conditions</td>
<td>• RADIUS:Service-Type equals Framed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RADIUS:NAS-Port-Type equals Wireless-IEEE802.11</td>
<td></td>
</tr>
<tr>
<td>Wired MAB Compound Condition</td>
<td>Policy &gt; Policy Elements &gt; Conditions &gt; Authentication &gt;</td>
<td>This compound condition checks for the following attributes and values:</td>
<td>This compound condition is used in the wired MAB authentication policy. Any request that matches the criteria specified in this policy would be evaluated based on the wired MAB authentication policy.</td>
</tr>
<tr>
<td></td>
<td>Compound Conditions</td>
<td>• RADIUS:Service-Type equals Call-Check</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RADIUS:NAS-Port-Type equals Ethernet</td>
<td></td>
</tr>
<tr>
<td>Catalyst Switch Local Web Authentication</td>
<td>Policy &gt; Policy Elements &gt; Conditions &gt; Authentication &gt;</td>
<td>This compound condition checks for the following attributes and values:</td>
<td>To use this compound condition, you must create an authentication policy that would check for this condition. You can also define an access service based on your requirements or use the default network access allowed protocols service for this policy.</td>
</tr>
<tr>
<td>Compound Condition</td>
<td>Compound Conditions</td>
<td>• RADIUS:Service-Type equals Outbound</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• RADIUS:NAS-Port-Type equals Ethernet</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Path in the User Interface</td>
<td>Description</td>
<td>Additional Information</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
</tbody>
</table>
| Wireless Lan Controller (WLC) Local Web Authentication Compound Condition | Policy > Policy Elements > Conditions > Authentication > Compound Conditions | This compound condition checks for the following attributes and values:  
- RADIUS:Service-Type equals Outbound  
- RADIUSNAS-Port-Type equals Wireless-IEEE802.11 | To use this compound condition, you must create an authentication policy that would check for this condition. You can also define an access service based on your requirements or use the default network access allowed protocols service for this policy. |
| Wired 802.1X Authentication Policy | Policy > Authentication > Rule-Based | This policy uses the wired 802.1X compound condition and the default network access allowed protocols service. This policy will evaluate requests that match the criteria specified in the wired 802.1X compound condition. | This default policy uses the internal endpoints database as its identity source. You can edit this policy to configure any identity source sequence or identity source based on your needs. |
| Wireless 802.1X Authentication Policy | Policy > Authentication > Rule-Based | This policy uses the wireless 802.1X compound condition and the default network access allowed protocols service. This policy will evaluate requests that match the criteria specified in the wireless 802.1X compound condition. | This default policy uses the internal endpoints database as its identity source. You can edit this policy to configure any identity source sequence or identity source based on your needs. |
| Wired MAB Authentication Policy | Policy > Authentication > Rule-Based | This policy uses the wired MAB compound condition and the default network access allowed protocols service. This policy will evaluate requests that match the criteria specified in the wired MAB compound condition. | This default policy uses the internal endpoints database as its identity source. |

Related Topics

- Network Access Service, on page 584
- Configure a Rule-Based Authentication Policy, on page 597
View Authentication Results

Cisco ISE provides various ways to view real-time authentication summary.

Before you begin
To perform the following task, you must be a Super Admin or System Admin.

Step 1
For network authentications (RADIUS), choose Operations > RADIUS > Live Logs or for device authentications (TACACS), choose Operations > TACACS > Live Logs to view the real-time authentication summaries.

Step 2
You can view the authentication summary in the following ways:

• Hover your mouse cursor over the Status icon to view the results of the authentication and a brief summary. A pop-up with status details appears.

• Enter your search criteria in any one or more of the text boxes that appear at the top of the list, and press Enter, to filter your results.

• Click the magnifier icon in the Details column to view a detailed report.

Note
As the Authentication Summary report or dashboard collects and displays the latest data corresponding to failed or passed authentications, the contents of the report appear after a delay of a few minutes.

Authentication Dashlet

The Cisco ISE dashboard provides a summary of all authentications that take place in your network and for your devices. It provides at-a-glance information about authentications and authentication failures in the Authentications dashlet.

The RADIUS Authentications dashlet provides the following statistical information about the authentications that Cisco ISE has handled:

• The total number of RADIUS authentication requests that Cisco ISE has handled, including passed authentications, failed authentications, and simultaneous logins by the same user.

• The total number of failed RADIUS authentications requests that Cisco ISE has processed.

You can also view a summary of TACACS+ authentications. The TACACS+ Authentications dashlet provides statistical information for device authentications.

For more information about device administration authentications, see TACACS Live Logs, on page 1159. For additional information about RADIUS Live Logs settings, see RADIUS Live Logs, on page 1153.

ISE Community Resource

For information on how to troubleshoot failed authentications and authorizations, see How To: Troubleshoot ISE Failed Authentications & Authorizations.
Authentication Reports and Troubleshooting Tools

Apart from the authentication details, Cisco ISE provides various reports and troubleshooting tools that you can use to efficiently manage your network.

There are various reports that you can run to understand the authentication trend and traffic in your network. You can generate reports for historical as well as current data. The following is a list of authentication reports:

- AAA Diagnostics
- RADIUS Accounting
- RADIUS Authentication
- Authentication Summary

You must enable IPv6 snooping on Cisco Catalyst 4000 Series switches, otherwise IPv6 address will not be mapped to the authentication sessions and will not be displayed in the show output. Use the following commands to enable IPv6 snooping:

```bash
vlan config <vlan-number>
  ipv6 snooping
  end
  ipv6 nd raguard policy router
  device-role router
  interface <access-interface>
    ipv6 nd raguard
  interface <uplink-interface>
    ipv6 nd raguard attach-policy router
  end
```
Manage Authorization Policies and Profiles

- Cisco ISE Authorization Policies, on page 607
- Cisco ISE Authorization Profiles, on page 607
- Default Authorization Policies, on page 611
- Configure Authorization Policies, on page 612
- Permissions for Authorization Profiles, on page 616
- Downloadable ACLs, on page 617
- Machine Access Restriction for Active Directory User Authorization, on page 618

Cisco ISE Authorization Policies

Authorization policies are a component of the Cisco ISE network authorization service. This service allows you to define authorization policies and configure authorization profiles for specific users and groups that access your network resources.

Authorization policies can contain conditional requirements that combine one or more identity groups using a compound condition that includes authorization checks that can return one or more authorization profiles. In addition, conditional requirements can exist apart from the use of a specific identity group (such as in using the default “Any”).

Authorization policies are used when creating authorization profiles in Cisco Identity Services Engine (Cisco ISE). An authorization policy is composed of authorization rules. Authorization rules have three elements: name, attributes, and permissions. The permission element is that maps to an authorization profile.

Cisco ISE Authorization Profiles

Authorization policies associate rules with specific user and group identities to create the corresponding profiles. Whenever these rules match the configured attributes, the corresponding authorization profile that grants permission is returned by the policy and network access is authorized accordingly.

For example, authorization profiles can include a range of permissions that are contained in the following types:

- Standard profiles
- Exception profiles
- Device-based profiles

Cisco Identity Services Engine Administrator Guide, Release 2.2
Profiles consist of attributes chosen from a set of resources, which are stored in any of the available vendor dictionaries, and these are returned when the condition for the specific authorization policy matches. Because authorization policies can include condition mapping to a single network service rule, these can also include a list of authorization checks.

Authorization verifications must comply with the authorization profiles to be returned. Authorization verifications typically comprise one or more conditions, including a user-defined name that can be added to a library, which can then be reused by other authorization policies.

Related Topics
- Authorization Policy Terminology, on page 608
- Authorization Policies and Supported Dictionaries, on page 610
- Configure Authorization Policies, on page 612
- Permissions for Authorization Profiles, on page 616
- Configure Permissions for Downloadable ACLs, on page 617

Authorization Policy Terminology

You can define authorization profiles and policies for network authorization of users to access Cisco ISE network and its resources. Cisco ISE also uses downloadable ACLs (DACLs), which are configured and implemented through authorization profiles. For more information about authorization profiles, see Authorization Profile, on page 608. For more information about DACLs, see Downloadable ACLs, on page 617.

Network Authorization

Network authorization controls user access to the network and its resources and what each user can do on the system with those resources. Activate network authorization from Cisco ISE by defining sets of permissions that authorize read, write, and execute privileges. Cisco ISE lets you create a number of different authorization policies to suit your network needs. This release supports only RADIUS access to the Cisco ISE network and its resources.

Policy Elements

Policy elements are components that define an authorization policy and are as follows:

- Rule name
- Identity groups
- Conditions
- Permissions

These policy elements are referenced when you create policy rules and your choice of conditions and attributes can create specific types of authorization profiles.

Authorization Profile

An authorization profile acts as a container where a number of specific permissions allow access to a set of network services. The authorization profile is where you define a set of permissions to be granted for a network access request and can include:
Authorization Policy

An authorization policy can consist of a single rule or a set of rules that are user-defined. These rules act to create a specific policy. For example, a standard policy can include the rule name using an If-Then convention that links a value entered for identity groups with specific conditions or attributes to produce a specific set of permissions that create a unique authorization profile. There are two authorization policy options you can set:

- First Matched Rules Apply
- Multiple Matched Rule Applies

These two options direct Cisco ISE to use either the first matched or the multiple matched rule type listed in the standard policy table when it matches the user’s set of permissions. These are the two types of authorization policies that you can configure:

- Standard—Standard policies are policies created to remain in effect for long periods of time, to apply to a larger group of users, devices, or groups, and to allow access to specific or all network endpoints. Standard policies are intended to be stable and apply to a large groups of users, devices, and groups that share a common set of privileges.

  Standard policies can be used as templates that you modify to serve the needs of a specific identity group, using specific conditions or permissions, to create another type of standard policy to meet the needs of new divisions, or user groups, devices, or network groups.

- Exception—By contrast, exception policies are appropriately named because this type of policy acts as an exception to the standard policies. Exception polices are intended for authorizing limited access that is based on a variety of factors, such as short-term policy duration, specific types of network devices, network endpoints or groups, or the need to meet special conditions or permissions or an immediate requirement.

  Exception policies are created to meet an immediate or short-term need, such as authorizing a limited number of users, devices, or groups to access network resources. An exception policy lets you create a specific set of customized values for an identity group, condition, or permission that are tailored for one user or a subset of users. This allows you to create different or customized policies to meet your corporate, group, or network needs.

Access Control Lists

An access control list (ACL) in the Cisco ISE system is a list of permissions attached to a specific object or network resource. An ACL specifies which users or groups are granted access to an object, as well as what operations are allowed on a given object or network resource. Each entry in a typical ACL specifies a subject and an operation or provides the state (such as, Permit or Deny).
Authorization Policies and Supported Dictionaries

For authorization policy types, the verification must comply with the authorization profiles to be returned. Verifications typically include one or more conditions that include a user-defined name that can then be added to a library and reused by other policies. You define conditions using the attributes from the Cisco ISE dictionary, which supports the following dictionaries:

- System-defined dictionary:
  - RADIUS

- RADIUS-vendor dictionaries
  - Airespace
  - Cisco
  - Cisco-BBSM
  - Cisco-VPN3000
  - Microsoft

Guidelines for Configuring Authorization Policies and Profiles

Observe the following guidelines when managing or administering authorization policies and profiles:

- Rule names you create must use only the following supported characters:
  - Symbols: plus (+), hyphen (-), underscore (_), period (.), and a space ( ).
  - Alphabetic characters: A-Z and a-z.

- Identity groups default to “Any” (you can use this global default to apply to all users).

- Conditions allow you to set one or more policy values. However, conditions are optional and are not required to create an authorization policy. These are the two methods for creating conditions:
  - Choose an existing condition or attribute from a corresponding dictionary of choices.
  - Create a custom condition that allows you to select a suggested value or use a text box to enter a custom value.

- Condition names you create must use only the following supported characters:
  - Symbols: hyphen (-), underscore (_), and period (.).
  - Alphabetic characters: A-Z and a-z.

- Permissions are important when choosing an authorization profile to use for a policy. A permission can grant access to specific resources or allow you to perform specific tasks. For example, if a user belongs to a specific identity group (such as Device Admins), and the user meets the defined conditions (such as
a site in Boston), then this user is granted the permissions associated with that group (such as access to a specific set of network resources or permission to perform a specific operation on a device).

# Default Authorization Policies

The Cisco ISE software comes with a number of pre-configured authorization rules that make it easier for you to create the authorization policies and profiles. These rules are disabled by default. You can enable these rules based on your requirements.

*Table 41: Pre-configured Authorization policies*

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Description</th>
<th>Conditions</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Black List Default</td>
<td>Blacklist AND Wireless_Access</td>
<td>Blackhole</td>
<td>Wireless_Access</td>
</tr>
<tr>
<td>Profiled Cisco IP Phones</td>
<td>Uses Cisco IP Phones as the default endpoint identity group.</td>
<td>Cisco_IP_Phone</td>
<td>Cisco_IP_Phone</td>
</tr>
<tr>
<td>Profiled Non Cisco IP Phones</td>
<td>Network_Access_Authentication_Passed AND Non_Compliant_Devices</td>
<td>DenyAccess</td>
<td>Non_Compliant_Devices</td>
</tr>
<tr>
<td>NonCompliant_Devices_Redirect</td>
<td>Deny access to authenticated devices that are not compliant.</td>
<td>Network_Access_Authentication_Passed AND Non_Compliant_Devices</td>
<td>AnyConnect_Temporal_Onboard</td>
</tr>
<tr>
<td>Unknown_Compliance_Redirect</td>
<td>Redirect authenticated devices with unknown posture status to the Client Provisioning Portal to access the AnyConnect Temporal Agent to check for compliance.</td>
<td>Network_Access_Authentication_Passed AND Compliance Unknown_Devices</td>
<td>AnyConnect_Temporal_Onboard</td>
</tr>
<tr>
<td>Compliant_Devices_Access</td>
<td>Compliant_Devices</td>
<td>PermitAccess</td>
<td>Compliant_Devices</td>
</tr>
<tr>
<td>Employee_EAP_TLS</td>
<td>Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN</td>
<td>PermitAccess AND BYOD</td>
<td></td>
</tr>
</tbody>
</table>
### Configure Authorization Policies

The Authorization Policy page lets you display, create, duplicate, modify, or delete authorization policies. The following authorization policy profile sections reference example actions directed at a standard authorization policy. You can follow the same process for managing an exception authorization policy.

**Before you begin**

Before you begin this procedure, you should have a basic understanding of simple and rule-based conditions, the basic building blocks of identity groups, conditions, and permissions, and how they are used in the Admin portal.

**Step 1** Choose **Policy > Authorization > Standard**.

**Step 2** Click the down arrow on the far-right and select either **Insert New Rule Above** or **Insert New Rule Below**.

**Step 3** Enter the rule name and select identity group, condition, attribute and permission for the authorization policy.

---

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Description</th>
<th>Conditions</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee_Onboarding</td>
<td>Any wireless 802.1X authentication that uses MSCHAPv2 would be redirected to the Native Supplicant Provisioning process.</td>
<td>(Wireless_802.1X AND EAP-MSCHAPv2)</td>
<td>NSP_Onboard AND BYOD</td>
</tr>
<tr>
<td>Wi-Fi_Guest_Access</td>
<td>To permit Guest access, after a Guest user is authenticated from the WebAuth.</td>
<td>(GuestType_Daily (default) OR GuestType_Weekly (default) OR GuestType_Contractor (default) ) AND (Wireless_MAB AND Guest_Flow)</td>
<td>Guest AND PermitAccess</td>
</tr>
<tr>
<td>Wi-Fi_Redirect_to_Guest_Login</td>
<td>To redirect users to the CWA Portal.</td>
<td>Wireless_MAB</td>
<td>Cisco_WebAuth</td>
</tr>
<tr>
<td>Basic_Authenticated_Access</td>
<td>To enable access to authenticated users.</td>
<td>Network_Access_Authentication_Pass</td>
<td>PermitAccess</td>
</tr>
<tr>
<td>Default</td>
<td>Deny access to devices that do not match the specified policy.</td>
<td>DenyAccess</td>
<td>DenyAccess</td>
</tr>
</tbody>
</table>

---

**Note**

The pre-configured authorization rules are available only on new installations. These rules are not available if you are upgrading from earlier versions of Cisco ISE.
Not all attributes you select will include the “Equals,” “Not Equals,” “Matches,” “Starts With,” or “Not Starts With” operator options.

The “Matches” operator supports and uses regular expressions (REGEX) not wildcards.

**Note** You must use the “equals” operator for straightforward comparison. “Contains” operator can be used for multi-value attributes. “Matches” operator should be used for regular expression comparison. When “Matches” operator is used, regular expression will be interpreted for both static and dynamic values.

**Step 4** Click Done.

**Step 5** Click Save to save your changes to the Cisco ISE system database and create this new authorization policy.

---

### Related Topics

- Create Simple Conditions, on page 558
- Create Compound Conditions, on page 559
- Simple and Compound Conditions, on page 557

---

### Authorization Policy Attributes and Conditions

To reuse a valid attribute when creating authorization policy conditions, select it from a dictionary that contains the supported attributes. For example, Cisco ISE provides an attribute named AuthenticationIdentityStore, which is located in the NetworkAccess dictionary. This attribute identifies the last identity source that was accessed during the authentication of a user:

- When a single identity source is used during authentication, this attribute includes the name of the identity store in which the authentication succeeded.
- When an identity source sequence is used during authentication, this attribute includes the name of the last identity source accessed.

You can use the AuthenticationStatus attribute in combination with the AuthenticationIdentityStore attribute to define a condition that identifies the identity source to which a user has successfully been authenticated. For example, to check for a condition where a user authenticated using an LDAP directory (LDAP13) in the authorization policy, you can define the following reusable condition:

```
If NetworkAccess.AuthenticationStatus EQUALS AuthenticationPassed AND
NetworkAccess.AuthenticationIdentityStore EQUALS LDAP13
```

**Note**

The AuthenticationIdentityStore represents a text field that allows you to enter data for the condition. Ensure that you enter or copy the name correctly into this field. If the name of the identity source changes, you must ensure to modify this condition to match the change to the identity source.

To define authorization conditions that are based on an endpoint identity group that has been previously authenticated, Cisco ISE supports authorization that was defined during endpoint identity group 802.1X authentication status. When Cisco ISE performs 802.1X authentication, it extracts the MAC address from the “Calling-Station-ID” field in the RADIUS request and uses this value to look up and populate the session cache for the device's endpoint identity group (defined as an endpointIDgroup attribute).
This process makes the endpoint ID group attribute available for use in creating authorization policy conditions, and allows you to define an authorization policy based on endpoint identity group information using this attribute, in addition to user information.

The condition for the endpoint identity group can be defined in the ID Groups column of the authorization policy configuration page. Conditions that are based on user-related information need to be defined in the “Other Conditions” section of the authorization policy. If user information is based on internal user attributes, then use the ID Group attribute in the internal user dictionary. For example, you can enter the full value path in the identity group using a value like “User Identity Group:Employee:US”.

ISE Community Resource

For an example of how to configure authorization policies in Cisco ISE based on SSIDs, see ISE Policies Based on SSID Configuration Example.

**Time and Date Conditions**

Use the Policy Elements Conditions page to display, create, modify, delete, duplicate, and search time and date policy element conditions. Policy elements are shared objects that define a condition that is based on specific time and date attribute settings that you configure.

Time and date conditions let you set or limit permission to access Cisco ISE system resources to specific times and days as directed by the attribute settings you make.

**Related Topics**

- Time and Date Condition Settings, on page 1115
- Create Time and Date Conditions, on page 568

**Use IPv6 Condition Attributes in Authorization Policies**

Cisco ISE can detect, manage, and secure IPv6 traffic from endpoints.

When an IPv6-enabled endpoint connects to the Cisco ISE network, it communicates with the Network Access Device (NAD) over an IPv6 network. The NAD conveys the accounting and profiling information from the endpoint (including IPv6 values) to Cisco ISE over an IPv4 network. You can configure authorization profiles and policies in Cisco ISE using the IPv6 attributes in your rule conditions in order to process such requests from IPv6-enabled endpoints and ensure that the endpoint is compliant.

Wildcard characters are supported in IPv6 prefix and IPv6 interface values. For example: 2001:db8:1234::/48.

Supported IPv6 address formats include:

- Full notation: Eight groups of four hexadecimal digits separated by colons. For example, 2001:0db8:85a3:0000:0000:0000:8a2e:0370:7334
- Shortened notation: Exclude leading zeros in a group; replace groups of zeros with two consecutive colons. For example: 2001:db8:85a3::8a2e:370:7334
- Dotted-quad notation (IPv4-mapped and IPv4 compatible-IPv6 addresses): For example, ::ffff:192.0.2.128

Supported IPv6 attributes include:

- NAS-IPv6-Address
- Framed-Interface-Id
Supported Cisco Attribute-Value pairs and their equivalent IETF attributes are listed in the table below:

<table>
<thead>
<tr>
<th>Cisco Attribute-Value Pairs</th>
<th>IETF Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv6:addrv6=&lt;ipv6 address&gt;</td>
<td>Framed-ipv6-Address</td>
</tr>
<tr>
<td>ipv6:stateful-ipv6-address-pool=&lt;name&gt;</td>
<td>Stateful-IPv6-Address-Pool</td>
</tr>
<tr>
<td>ipv6:delegated-ipv6-pool=&lt;name&gt;</td>
<td>Delegated-IPv6-Prefix-Pool</td>
</tr>
<tr>
<td>ipv6:ipv6-dns-servers-addr=&lt;ipv6 address&gt;</td>
<td>DNS-Server-IPv6-Address</td>
</tr>
</tbody>
</table>

The RADIUS Live Logs page, RADIUS Authentication report, RADIUS Accounting report, Current Active Session report, RADIUS Error report, Misconfigured NAS report, EPS Audit report, and Misconfigured Supplicant reports support IPv6 addresses. You can view the details about these sessions from the RADIUS Live Logs page or from any of these reports. You can filter the records based on IPv4, IPv6, or MAC addresses.

Note

If you connect an Android device to an IPv6 enabled DHCPv6 network, it receives only the link-local IPv6 address from the DHCP server. Hence, global IPv6 address is not displayed in the Live Logs and in the Endpoints page (Work Centers > Network Access > Identities > Endpoints).

The following procedure describes how to configure IPv6 attributes in authorization policies.

**Before you begin**

Ensure that the NADs in your deployment support AAA with IPv6. Refer to AAA Support for IPv6 for information on how to enable AAA support for IPv6 on your NADs.

**Step 1**  
For network access policies, choose Work Centers > Network Access > Policy Sets. For device administration policies, choose Work Centers > Device Administration > Device Admin Policy Sets.

**Step 2**  
Create authorization rules.

**Step 3**  
When creating authorization rules, create a condition from the Conditon Studio. In the Condition Studio, from the RADIUS dictionary, choose the RADIUS IPv6 attribute, the operator, and the value.
Permissions for Authorization Profiles

Before you start configuring permissions for authorization profiles, make sure you:

- Understand the relationship between authorization policies and profiles
- Are familiar with the Authorization Profile page
- Know the basic guidelines to follow when configuring policies and profiles
- Understand what comprises permissions in an authorization profile

To work with Authorization Profiles, choose Policy > Policy Elements > Results. From the menu on the left, choose Authorization > Authorization Profiles.

Use the Results navigation pane as your starting point in the process for displaying, creating, modifying, deleting, duplicating, or searching policy element permissions for the different types of authorization profiles on your network. The Results pane initially displays Authentication, Authorization, Profiling, Posture, Client Provisioning, and Trustsec options.

Authorization profiles let you choose the attributes to be returned when a RADIUS request is accepted. Cisco ISE provides a mechanism where you can configure Common Tasks settings to support commonly-used attributes. You must enter the value for the Common Tasks attributes, which Cisco ISE translates to the underlying RADIUS values.

ISE Community Resource

For an example of how to configure Media Access Control Security (MACsec) encryption between an 802.1x supplicant (Cisco AnyConnect Mobile Security) and an authenticator (switch), see MACsec Switch-host Encryption with Cisco AnyConnect and ISE Configuration Example.

Related Topics

- Authorization Policies and Supported Dictionaries, on page 610
- Guidelines for Configuring Authorization Policies and Profiles, on page 610
- Configure Permissions for New Standard Authorization Profiles, on page 616

Configure Permissions for New Standard Authorization Profiles

Step 1 Choose Policy > Policy Elements > Results > Authorization > Authorization Profiles.
Step 2 Click Add.
Step 3 Enter values as required to configure a new authorization profile. Supported characters for the name field are: space, ! # $ % & ' ( ) * + , - . / ; = ? @ _ { }. Once you configure the profile, you can double-check the RADIUS syntax from the Attributes Details that dynamically appear at the bottom of the screen.
Step 4 Click Submit to save your changes to the Cisco ISE system database to create an authorization profile.
Access control lists (ACLs) are lists of access control entries (ACEs), which may be applied by a Policy Enforcement Point (for example, a switch) to a resource. Each ACE identifies the permissions allowed per user for that object, such as read, write, execute and more. For example, an ACL may be configured for use the Sales area of the network, with an ACE allowing Write permissions for the Sales group and a separate ACE allowing Read permissions for all other employees of the organization. With RADIUS protocol, ACLs grant authorization by filtering source and destination IP addresses, transport protocols, and additional parameters. Static ACLs reside on and are directly configured from the switch and can be applied in your authorization policies from the ISE GUI; downloadable ACLs (DACLs) can be configured, managed and applied in your authorization policies from the ISE GUI.

To implement DACLs in your network authorization policy in ISE:

1. Configure a new or existing DACL from Policy > Policy Elements > Results > Downloadable ACLs. For more information see Configure Permissions for Downloadable ACLs, on page 617.

2. Configure a new or existing authorization profile from Policy > Policy Elements > Results > Authorization Profiles, using any of the DACLs you already configured.

3. Implement the authorization profiles you have configured when creating and configuring new and existing policy sets from Policy > Policy Sets.

### Configure Permissions for Downloadable ACLs

With ISE, downloadable ACLs (DACLs) can be configured and implemented in your authorization policies for control of how the network is accessed by different users and groups of users. Default authorization DACLs are available with installation of ISE, including the following default profiles:

- DENY_ALL_TRAFFIC
- PERMIT_ALL_TRAFFIC

When working with DACLs, these defaults cannot be changed, but you can duplicate them in order to create additional, similar, DACLs.

---

**Step 1** Choose Policy > Policy Elements > Results > Authorization > Downloadable ACLs.

**Step 2** Click Add from the top of the Downloadable ACLs table or alternatively, choose any of the existing DACLs and click Duplicate from the top of the table.

**Step 3** Enter or edit the desired values for the DACL, keeping in mind the following rules:

- Supported characters for the name field are: alphanumeric, hyphen(-), dot(.) and underscore(_).

- The keyword Any must be the source in all ACEs in the DACL. Once the DACL is pushed, the Any in the source is replaced with the IP address of the client that is connecting to the switch.
**Step 4** Optionally, when you finish creating the complete list of ACEs, click **Check DACL Syntax** to validate the list. If there are validation errors, the check returns specific instructions identifying the invalid syntax in the window that opens automatically.

**Step 5** Click **Submit**.

---

**Related Topics**

- **Configure Permissions for Downloadable ACLs**, on page 617

---

**Machine Access Restriction for Active Directory User Authorization**

Cisco ISE contains a Machine Access Restriction (MAR) component that provides an additional means of controlling authorization for Microsoft Active Directory-authentication users. This form of authorization is based on the machine authentication of the computer used to access the Cisco ISE network. For every successful machine authentication, Cisco ISE caches the value that was received in the RADIUS Calling-Station-ID attribute (attribute 31) as evidence of a successful machine authentication.

Cisco ISE retains each Calling-Station-ID attribute value in cache until the number of hours that was configured in the “Time to Live” parameter in the Active Directory Settings page expires. Once the parameter has expired, Cisco ISE deletes it from its cache.

When a user authenticates from an end-user client, Cisco ISE searches the cache for a Calling-Station-ID value from successful machine authentications for the Calling-Station-ID value that was received in the user authentication request. If Cisco ISE finds a matching user-authentication Calling-Station-ID value in the cache, this affects how Cisco ISE assigns permissions for the user that requests authentication in the following ways:

- If the Calling-Station-ID value matches one found in the Cisco ISE cache, then the authorization profile for a successful authorization is assigned.

- If the Calling-Station-ID value is not found to match one in the Cisco ISE cache, then the authorization profile for a successful user authentication without machine authentication is assigned.
CHAPTER 22

Configure Threat Centric NAC Service

- Threat Centric NAC Service, on page 619

Threat Centric NAC Service

Threat Centric Network Access Control (TC-NAC) feature enables you to create authorization policies based on the threat and vulnerability attributes received from the threat and vulnerability adapters. Threat severity levels and vulnerability assessment results can be used to dynamically control the access level of an endpoint or a user.

You can configure the vulnerability and threat adapters to send high fidelity Indications of Compromise (IoC), Threat Detected events, and CVSS scores to Cisco ISE, so that threat-centric access policies can be created to change the privilege and context of an endpoint accordingly.

Cisco ISE supports the following adapters:

- SourceFire FireAMP
- Cognitive Threat Analytics (CTA) adapter
- Qualys

Note

Only the Qualys Enterprise Edition is currently supported for TC-NAC flows.

- Rapid7 Nexpose
- Tenable Security Center

When a threat event is detected for an endpoint, you can select the MAC address of the endpoint on the Compromised Endpoints page and apply an ANC policy, such as Quarantine. Cisco ISE triggers CoA for that endpoint and applies the corresponding ANC policy. If ANC policy is not available, Cisco ISE triggers CoA for that endpoint and applies the original authorization policy. You can use the Clear Threat and Vulnerabilities option on the Compromised Endpoints page to clear the threat and vulnerabilities associated with an endpoint (from Cisco ISE system database).

The following attributes are listed under the Threat dictionary:

- CTA-Course_Of_Action (values can be Internal Blocking, Eradication, or Monitoring)
The valid range is from 0 to 10 for both Base Score and Temporal Score attributes. When a vulnerability event is received for an endpoint, Cisco ISE triggers CoA for that endpoint. However, CoA is not triggered when a threat event is received.

You can create an authorization policy by using the vulnerability attributes to automatically quarantine the vulnerable endpoints based on the attribute values. For example:

Any Identity Group & Threat: Qualys-CVSS_Base_Score > 7.0 -> Quarantine

Note the following points while enabling the Threat Centric NAC service:

- The Threat Centric NAC service requires an Apex license.
- Threat Centric NAC service can be enabled on only one node in a deployment.
- You can add only one instance of an adapter per vendor for Vulnerability Assessment service. However, you can add multiple instances of FireAMP adapter.
- You can stop and restart an adapter without losing its configuration. After configuring an adapter, you can stop the adapter at any point of time. The adapter would remain in this state even when the ISE services are restarted. Select the adapter and click Restart to start the adapter again.

Note

When an adapter is in Stopped state, you can edit only the name of the adapter instance; you cannot edit the adapter configuration or the advanced settings.

The Threat Centric NAC Live Logs page (Operations > TC NAC Live Log) lists all the threat and vulnerability events. It displays the incident type, adapter name, matching authorization rule, and authorization profiles (old and new) for an endpoint. You can also view the detailed information for an event.

You can view the threat information for the endpoints on the following pages:

- Home page > Threat dashboard
- Context Visibility > Endpoints > Compromised Endpoints

The following alarms are triggered by the Threat Centric NAC service:

- Adapter not reachable (syslog ID: 91002)—Indicates that the adapter cannot be reached.
- Adapter Connection Failed (syslog ID: 91018)—Indicates that the adapter is reachable but the connection between the adapter and source server is down.
- Adapter Stopped Due to Error (syslog ID: 91006)—This alarm is triggered if the adapter is not in the desired state. If this alarm is displayed, check the adapter configuration and server connectivity. Refer to the adapter logs for more details.
• Adapter Error (syslog ID: 91009)—Indicates that the Qualys adapter is unable to establish a connection with or download information from the Qualys site.

The following reports are available for the Threat Centric NAC service:
• Adapter Status—The Adapter Status report displays the status of the threat and vulnerability adapters.
• COA Events—When a vulnerability event is received for an endpoint, Cisco ISE triggers CoA for that endpoint. The CoA Events report displays the status of these CoA events. It also displays the old and new authorization rules and the profile details for these endpoints.
• Threat Events—The Threat Events report provides a list of all the threat events that Cisco ISE receives from the various adapters that you have configured. Vulnerability Assessment events are not included in this report.
• Vulnerability Assessment—The Vulnerability Assessment report provides information about the assessments that are happening for your endpoints. You can view this report to check if the assessment is happening based on the configured policy.

You can view the following information from Operations > Reports > Diagnostics > ISE Counters > Threshold Counter Trends:
• Total number of events received
• Total number of threat events
• Total number of vulnerability events
• Total number of CoAs issued (to PSN)

The values for these attributes are collected every 5 minutes, so these values represent the count for the last 5 minutes.

The Threat dashboard contains the following dashlets:
• Total Compromised Endpoints dashlet displays the total number of endpoints (both connected and disconnected endpoints) that are currently impacted on the network.
• Compromised Endpoints Over Time dashlet displays a historical view of the impact on endpoints for the specified time period.
• Top Threats dashlet displays the top threats based on the number of endpoints impacted and the severity of the threat.
• You can use the Threats Watchlist dashlet to analyze the trend of selected events.

The size of the bubbles in the Top Threats dashlet indicates the number of endpoints impacted and the light shaded area indicates the number of disconnected endpoints. The color as well as the vertical scale indicate the severity of the threat. There are two categories of threat—Indicators and Incidents. The severity attribute for Indicator is "Likely_Impact" and the severity attribute for Incident is "Impact_Qualification".

The Compromised Endpoint page displays the matrix view of the endpoints that are impacted and the severity of the impact for each threat category. You can click on the device link to view the detailed threat information for an endpoint.

The Course Of Action chart displays the action taken (Internal Blocking, Eradication, or Monitoring) for the threat incidents based on the CTA-Course_Of_Action attribute received from the CTA adapter.
The Vulnerability dashboard on the Home page contains the following dashlets:

- **Total Vulnerable Endpoints dashlet** displays the total number of endpoints that have a CVSS score greater than the specified value. Also displays the total number of connected and disconnected endpoints that have a CVSS score greater than the specified value.

- **Top Vulnerability dashlet** displays the top vulnerabilities based on the number of endpoints impacted or the severity of the vulnerability. The size of the bubbles in the Top Vulnerability dashlet indicates the number of endpoints impacted and the light shaded area indicates the number of disconnected endpoints. The color as well as the vertical scale indicates the severity of the vulnerability.

- **You can use the Vulnerability Watchlist dashlet** to analyze the trend of selected vulnerabilities over a period of time. Click the search icon in the dashlet and enter the vendor-specific id ("qid" for Qualys ID number) to select and view the trend for that particular ID number.

- **The Vulnerable Endpoints Over Time dashlet** displays a historical view of the impact on endpoints over time.

The Endpoint Count By CVSS graph on the Vulnerable Endpoints page shows the number of endpoints that are affected and their CVSS scores. You can also view the list of affected endpoints on the Vulnerable Endpoints page. You can click on the device link to view the detailed vulnerability information for each endpoint.

Threat Centric NAC service logs are included in the support bundle (see Download Cisco ISE Log Files, on page 897). Threat Centric NAC service logs are located at support/logs/TC-NAC/.

### Enable Threat Centric NAC Service

To configure vulnerability and threat adapters, you must first enable the Threat Centric NAC service. This service can be enabled on only one Policy Service Node in your deployment.

**Step 1** Choose Administration > System > Deployment.

**Step 2** Check the box next to the PSN on which you want to enable the Threat Centric NAC service and click Edit.

**Step 3** Check the Enable Threat Centric NAC Service check box.

**Step 4** Click Save.

**Related Topics**

- Add SourceFire FireAMP Adapter, on page 622
- Configure Cognitive Threat Analytics Adapter, on page 623
- Configure Authorization Profiles for CTA Adapter, on page 625
- Configure Authorization Policy using the Course of Action Attribute, on page 625
- Threat Centric NAC Service, on page 619

### Add SourceFire FireAMP Adapter

**Before you begin**

- You must have an account with SourceFire FireAMP.
- You must deploy FireAMP clients on all endpoints.
Configure Cognitive Threat Analytics Adapter

**Before you begin**

- You must enable Threat Centric NAC service on the deployment node (see Enable Threat Centric NAC Service, on page 622).
- Log in to Cisco Cognitive Threat Analytics (CTA) portal via http://cognitive.cisco.com/login and request CTA STIX/TAXII service. For more information, see Cisco ScanCenter Administrator Guide.
• Cognitive Threat Analytics (CTA) adapter uses TAXII protocol with SSL to poll the CTA cloud for detected threats. It also supports the use of proxy.

• Import the adapter certificate into the Trusted Certificate Store. Choose Administration > System > Certificates > Trusted Certificates > Import to import the certificate.

---

**Step 1**
Choose Administration > Threat Centric NAC > Third Party Vendors.

**Step 2**
Click Add.

**Step 3**
Select CTA: Threat from the Vendor drop-down list.

**Step 4**
Enter a name for the adapter instance.

**Step 5**
Click Save.

**Step 6**
Refresh the Vendor Instances listing page. You can configure the adapter only after the adapter status changes to Ready to Configure on the Vendor Instances listing page.

**Step 7**
Click the Ready to configure link.

**Step 8**
Enter the following details:

- CTA STIX/TAXII service URL—URL of the CTA cloud service. By default, the following URL is used: https://taxii.cloudsec.sco.cisco.com/skym-taxii-ws/PollService/

- CTA feed name—Enter the feed name of the CTA cloud service.

- CTA username and password—Enter the username and password for the CTA cloud service.

- Proxy host and port (optional)—If you have configured a proxy server to route all the traffic, enter the hostname and the port number of the proxy server.

- Polling interval—Time interval between each poll. Default value is 30 minutes.

- First Poll Duration in hours—Age of the data to be pulled at the first poll. Default value is 2 hours. Maximum value is 12 hours.

- Incident Type—The following options are available:
  - CTA events only
  - AMP events only
  - CTA and AMP events

**Step 9**
Click Next.

**Step 10**
Click Advanced Settings to configure the following options:

- Impact Qualification—Select the severity level of the incident to be polled. The following options are available:
  - 1 - Insignificant
  - 2 - Distracting
  - 3 - Painful
  - 4 - Damaging
  - 5 - Catastrophic
For example, if you have selected "3-Painful", incidents with this severity level (3-Painful) and above (in this case, 4-Damaging and 5-Catastrophic) are polled.

- Logging level—Choose a log level for the adapter. The available options are: Error, Info, and Debug.

**Step 11**

Click **Finish**.

---

**Note**

CTA works with user identities listed in the web proxy logs as IP addresses or usernames. Specifically, in the case of IP addresses, the IP address of a device that is available through the proxy logs may collide with the IP address of another device on the internal network. For example, roaming users connected via AnyConnect and a split-tunnel directly to the internet could acquire a local IP range address (for example, 10.0.0.X address), which may collide with an address in an overlapping private IP range used in an internal network. We recommend that you take into account the logical network architecture while defining the policies to avoid quarantine actions being applied on mismatched devices.

---

**Configure Authorization Profiles for CTA Adapter**

For each threat event, the CTA adapter returns one of the following values for the Course of Action attribute: Internal Blocking, Monitoring, or Eradication. You can create authorization profiles based on these values.

**Step 1**

Choose **Policy > Policy Elements > Authorization > Authorization Profiles**.

**Step 2**

Click **Add**.

**Step 3**

Enter a name and description for the authorization profile.

**Step 4**

Select the Access Type.

**Step 5**

Enter the required details and click **Submit**.

---

**Configure Authorization Policy using the Course of Action Attribute**

You can use the CTA-Course_Of_Action attribute to configure authorization policies for the endpoints for which threat events are reported. This attribute is available in the Threat directory.

You can also create exception rules based on the CTA-Course_Of_Action attribute.

**Step 1**

Choose **Policy > Policy Sets**

You can edit an existing policy rule or create a new exception rule for the endpoints with threat events.

**Step 2**

Create a condition to check for the CTA-Course_Of_Action attribute value and assign the appropriate authorization profile. For example:

```
Network_Access_Authentication_Passed AND ThreatCTA-Course_Of_Action CONTAINS Internal Blocking then blocking (authorization profile)
```

**Note**

"Internal Blocking" is the recommended Course of Action attribute to be used for quarantining the endpoints.
Step 3  Click Save.

When a threat event is received for an endpoint, Cisco ISE checks if there is any matching authorization policy for the endpoint and triggers CoA only if the endpoint is active. If the endpoint is offline, threat event details are added to the Threat Events report (Operations > Reports > Threat Centric NAC > Threat Events).

Note

Sometimes CTA sends multiple risks and their associated Course of Action attributes in one incident. For example, it can send "Internal Blocking" and "Monitoring" (course of action attributes) in one incident. In this case, if you have configured an authorization policy to quarantine endpoints using "equals" operator, the endpoints will not be quarantined. For example:

CTA-Course_Of_Action EQUALS Internal Blocking then Quarantine_Systems (authorization profile)

In such cases, you must use "contains" operator in the authorization policy to quarantine the endpoints. For example:

CTA-Course_Of_Action CONTAINS Internal Blocking then Quarantine_Systems

Support for Vulnerability Assessment in Cisco ISE

Cisco Identity Services Engine integrates with the following Vulnerability Assessment (VA) Ecosystem Partners to obtain vulnerability results of endpoints that connect to the Cisco ISE network:

• Qualys—Qualys is a cloud-based assessment system with scanner appliances deployed in the network. Cisco ISE allows you to configure an adapter that communicates with Qualys and obtains the VA results. You can configure the adapter from the Admin portal. You need a Cisco ISE administrator account with Super Admin privileges to configure the adapter. The Qualys adapter uses REST APIs to communicate with the Qualys Cloud Service. You need a user account in Qualys with Manager privileges to access the REST APIs. Cisco ISE uses following Qualys REST APIs:
  • Host Detection List API—To check the last scan results of the endpoint
  • Scan API—To trigger an on-demand scan of the endpoint

Qualys enforces limits on the number of API calls that subscribed users can make. The default rate limit count is 300 per 24 hours. Cisco ISE uses Qualys API version 2.0 to connect to Qualys. Refer to the Qualys API V2 User Guide for more information on these API functions.

• Rapid7 Nexpose—Cisco ISE integrates with Rapid 7 Nexpose, a vulnerability management solution, to help detect vulnerabilities and enables you to respond to such threats quickly. Cisco ISE receives the vulnerability data from Nexpose and based on the policies that you configure in ISE, it quarantines the affected endpoints. From the Cisco ISE dashboard, you can view the affected endpoint and take appropriate action.

Cisco ISE has been tested with Nexpose Release 6.4.1.

• Tenable Security Center (Nessus scanner)—Cisco ISE integrates with Tenable SecurityCenter and receives the vulnerability data from Tenable Nessus scanner (managed by Tenable SecurityCenter) and based on the policies that you configure in ISE, it quarantines the affected endpoints. From the Cisco ISE dashboard, you can view the affected endpoints and take appropriate action.

Cisco ISE has been tested with Tenable SecurityCenter 5.3.2.
The results from the ecosystem partner are converted in to a Structured Threat Information Expression (STIX) representation and based on this value, a Change of Authorization (CoA) is triggered, if needed, and the appropriate level of access is granted to the endpoint.

The time taken to assess endpoints for vulnerabilities depends on various factors and hence VA cannot be performed in real time. The factors that affect the time taken to assess an endpoint for vulnerabilities include:

- Vulnerability assessment ecosystem
- Type of vulnerabilities scanned for
- Type of scans enabled
- Network and system resources allocated by the ecosystem for the scanner appliances

In this release of Cisco ISE, only endpoints with IPv4 addresses can be assessed for vulnerabilities.

### Enable and Configure Vulnerability Assessment Service

To enable and configure Vulnerability Assessment Service in Cisco ISE, perform the following tasks:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Enable Threat Centric NAC Service, on page 622.</td>
</tr>
</tbody>
</table>
| Step 2 | To configure:  
  - Qualys adapter, see Configure Qualys Adapter, on page 628.  
  - Nexpose adapter, see Configure Nexpose Adapter, on page 630.  
  - Tenable adapter, see Configure Tenable Adapter, on page 632. |
| Step 3 | Configure Authorization Profile, on page 634. |
| Step 4 | Configure Exception Rule to Quarantine a Vulnerable Endpoint, on page 635. |

### Enable Threat Centric NAC Service

To configure vulnerability and threat adapters, you must first enable the Threat Centric NAC service. This service can be enabled on only one Policy Service Node in your deployment.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Administration &gt; System &gt; Deployment.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Check the check box next to the PSN on which you want to enable the Threat Centric NAC service and click Edit.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Check the Enable Threat Centric NAC Service check box.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Add SourceFire FireAMP Adapter, on page 622
- Configure Cognitive Threat Analytics Adapter, on page 623
- Configure Authorization Profiles for CTA Adapter, on page 625
- Configure Authorization Policy using the Course of Action Attribute, on page 625
- Threat Centric NAC Service, on page 619
Configure Qualys Adapter

Cisco ISE supports the Qualys Vulnerability Assessment Ecosystem. You must create a Qualys adapter for Cisco ISE to communicate with Qualys and obtain the VA results.

**Before you begin**

- You must have the following user accounts:
  - Admin user account in Cisco ISE with Super Admin privileges to be able to configure a vendor adapter.
  - User account in Qualys with Manager privileges

- Ensure that you have appropriate Qualys license subscriptions. You need access to the Qualys Report Center, Knowledge Base (KBX), and API. Contact your Qualys Account Manager for details.

- Import the Qualys server certificate into the Trusted Certificates store in Cisco ISE (Administration > Certificates > Certificate Management > Trusted Certificates > Import). Ensure that the appropriate root and intermediate certificates are imported (or present) in the Cisco ISE Trusted Certificates store.

- Refer to the Qualys API Guide for the following configurations:
  - Ensure that you have enabled CVSS Scoring in Qualys (Reports > Setup > CVSS Scoring > Enable CVSS Scoring).
  - Ensure that you add the IP address and subnet mask of your endpoints in Qualys (Assets > Host Assets).
  - Ensure that you have the name of the Qualys option profile. The option profile is the scanner template that Qualys uses for scanning. We recommend that you use an option profile that includes authenticated scans (this option checks the MAC Address of the endpoint as well).

- Cisco ISE communicates with Qualys over HTTPS/SSL (port 443).

---

**Step 1** Choose Administration > Threat Centric NAC > Third Party Vendors.

**Step 2** Click Add.

**Step 3** From the Vendor drop-down list, choose Qualys:VA.

**Step 4** Enter a name for the adapter instance. For example, Qualys_Instance.

The listing page appears with a list of configured adapter instances.

**Step 5** Refresh the Vendor Instances listing page. The status for the newly added Qualys_Instance adapter should change to Ready to Configure.

**Step 6** Click the Ready to Configure link.

**Step 7** Enter the following values in the Qualys configuration screen and click Next.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REST API Host</td>
<td>The hostname of the server that hosts the Qualys cloud. Contact your Qualys representative for this information.</td>
</tr>
<tr>
<td>REST API Port</td>
<td>443</td>
</tr>
</tbody>
</table>
Enable and Configure Cisco ISE Services

Configure Qualys Adapter

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>User account in Qualys with Manager privileges.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the Qualys user account.</td>
</tr>
<tr>
<td>HTTP Proxy Host</td>
<td>If you have a proxy server configured to route all Internet traffic, enter the hostname of the proxy server.</td>
</tr>
<tr>
<td>HTTP Proxy Port</td>
<td>Enter the port number used by the proxy server.</td>
</tr>
</tbody>
</table>

If the connection to the Qualys server is established, the Scanner Mappings page appears with a list of Qualys scanners. The Qualys scanners from your network appear in this page.

**Step 8**
Choose the default scanner that Cisco ISE will use for on-demand scans.

**Step 9**
In the PSN to Scanner Mapping area, choose one or more Qualys scanner appliance(s) to the PSN node, and click **Next**. The Advanced Settings page appears.

**Step 10**
Enter the following values in the Advanced Settings page. The settings in this page determine whether an on-demand scan will be triggered or the last scan results will be used for VA.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Option Profile</td>
<td>Choose the option profile that you want Qualys to use for scanning the endpoint. You can choose the default option profile, Initial Options.</td>
</tr>
<tr>
<td>Last Scan Results - Check Settings</td>
<td></td>
</tr>
<tr>
<td>Last scan results check interval in minutes</td>
<td>(Impacts the access rate of Host Detection List API) Time interval in minutes after which the last scan results must be checked again. Valid range is between 1 and 2880.</td>
</tr>
<tr>
<td>Maximum results before last scan results are checked</td>
<td>(Impacts the access rate of Host Detection List API) If the number of queued scan requests exceeds the maximum number specified here, the last scan results are checked before the time interval specified in <strong>Last scan results check interval in minutes</strong> field. Valid range is between 1 and 1000.</td>
</tr>
<tr>
<td>Verify MAC address</td>
<td>True or False. When set to true, the last scan results from Qualys would be used only if it includes the MAC address of the endpoint.</td>
</tr>
<tr>
<td>Scan Settings</td>
<td></td>
</tr>
<tr>
<td>Scan trigger interval in minutes</td>
<td>(Impacts the access rate of Scan API) Time interval in minutes after which an on-demand scan is triggered. Valid range is between 1 and 2880.</td>
</tr>
<tr>
<td>Maximum requests before scan is triggered</td>
<td>(Impacts the access rate of Scan API) If the number of queued scan requests exceeds the maximum number specified here, an on-demand scan would be triggered before the time interval specified in <strong>Scan trigger interval in minutes</strong> field. Valid range is between 1 and 1000.</td>
</tr>
<tr>
<td>Scan status check interval in minutes</td>
<td>Time interval in minutes after which Cisco ISE communicates with Qualys to check the status of the scan. Valid range is between 1 and 60.</td>
</tr>
</tbody>
</table>
Configure Nexpose Adapter

You must create a Nexpose adapter for Cisco ISE to communicate with Nexpose and obtain the VA results.

**Before you begin**

- Ensure that you have enabled the Threat-Centric NAC service in Cisco ISE.
- Log in to Nexpose Security Console and create a user account with the following privileges:
  - Manage sites
  - Create reports
- Import the Nexpose server certificate into the Trusted Certificates store in Cisco ISE (Administration > Certificates > Certificate Management > Trusted Certificates > Import). Ensure that the appropriate root and intermediate certificates are imported (or present) in the Cisco ISE Trusted Certificates store.
- Cisco ISE communicates with Nexpose over HTTPS/SSL (port 3780).

**Step 1** Choose Administration > Threat Centric NAC > Third Party Vendors.

**Step 2** Click Add.

**Step 3** From the Vendor drop-down list, choose Rapid7 Nexpose:VA.

**Step 4** Enter a name for the adapter instance. For example, Nexpose.

The listing page appears with a list of configured adapter instances.

**Step 5** Refresh the Vendor Instances listing page. The status for the newly added Nexpose adapter should change to Ready to Configure.
Step 6  Click the **Ready to Configure** link.

Step 7  Enter the following values in the Nexpose configuration screen and click **Next**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nexpose Host</td>
<td>The hostname of the Nexpose server.</td>
</tr>
<tr>
<td>Nexpose Port</td>
<td>3780.</td>
</tr>
<tr>
<td>Username</td>
<td>Nexpose Admin user account.</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the Nexpose Admin user account.</td>
</tr>
<tr>
<td>HTTP Proxy Host</td>
<td>If you have a proxy server configured to route all Internet traffic, enter the hostname of the proxy server.</td>
</tr>
<tr>
<td>HTTP Proxy Port</td>
<td>Enter the port number used by the proxy server.</td>
</tr>
</tbody>
</table>

Step 8  Click **Next** to configure Advanced Settings.

Step 9  Enter the following values in the Advanced Settings page. The settings in this page determine whether an on-demand scan will be triggered or the last scan results will be used for VA.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings for checking latest scan results</strong></td>
<td></td>
</tr>
<tr>
<td>Interval between checking the latest scan results in minutes</td>
<td>Time interval in minutes after which the last scan results must be checked again. Valid range is between 1 and 2880.</td>
</tr>
<tr>
<td>Number of pending requests that can trigger checking the latest scan results</td>
<td>If the number of queued scan requests exceeds the maximum number specified here, the last scan results are checked before the time interval specified in <strong>Interval between checking the latest scan results in minutes</strong> field. Valid range is between 1 and 1000.</td>
</tr>
<tr>
<td>Verify MAC address</td>
<td>True or False. When set to true, the last scan results from Nexpose would be used only if it includes the MAC address of the endpoint.</td>
</tr>
<tr>
<td><strong>Scan settings</strong></td>
<td></td>
</tr>
<tr>
<td>Scan trigger interval for each site in minutes</td>
<td>Time interval in minutes after which a scan is triggered. Valid range is between 1 and 2880.</td>
</tr>
<tr>
<td>Number of pending requests before a scan is triggered for each site</td>
<td>If the number of queued scan requests exceeds the maximum number specified here, a scan would be triggered before the time interval specified in <strong>Scan timeout in minutes</strong> field. Valid range is between 1 and 1000.</td>
</tr>
<tr>
<td>Scan timeout in minutes</td>
<td>Time in minutes after which the scan request will time out. If a scan request times out, an alarm is generated. Valid range is between 20 and 1440.</td>
</tr>
</tbody>
</table>
### Configure Tenable Adapter

You must create a Tenable adapter for Cisco ISE to communicate with Tenable SecurityCenter (Nessus scanner) and obtain the VA results.

**Before you begin**

- You must have Tenable Security Center and Tenable Nessus Vulnerability Scanner installed. While registering the Tenable Nessus scanner, ensure that you choose Managed by SecurityCenter in the Registration field.
- Create a user account with Security Manager privilege in Tenable SecurityCenter.
- Create a repository in SecurityCenter (Log in to Tenable SecurityCenter with Admin credentials and choose Repository > Add).
- Add the endpoint IP range to be scanned in the repository.
- Add Nessus scanner.
- Create scan zones and assign IP addresses to the scan zones and scanners that are mapped to these scan zones.
- Create a scan policy for ISE.
- Add an active scan and associate it with the ISE scan policy. Configure settings, targets (IP/DNS names).

---

**Step 10**

Click **Next** to review the Configuration Settings.

**Step 11**

Click **Finish**.

---

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Settings for checking latest scan results</strong></td>
<td></td>
</tr>
<tr>
<td>Number of sites for which scans could be triggered concurrently</td>
<td>The number of sites for which scans can be run concurrently. Valid range is between 1 and 200.</td>
</tr>
<tr>
<td>Timezone</td>
<td>Choose the time zone based on the time zone that is configured in the Nexpose server.</td>
</tr>
<tr>
<td>Http timeout in seconds</td>
<td>Time interval in seconds for Cisco ISE to wait for a response from Nexpose. Valid range is between 5 and 1200.</td>
</tr>
<tr>
<td>Choose the log level for adapter log files</td>
<td>Choose a log level for the adapter. The available options are ERROR, INFO, DEBUG, and TRACE.</td>
</tr>
</tbody>
</table>
• Export System and Root certificates from Tenable SecurityCenter and import it in to the Trusted Certificates store in Cisco ISE (Administration > Certificates > Certificate Management > Trusted Certificates > Import). Ensure that the appropriate root and intermediate certificates are imported (or present) in the Cisco ISE Trusted Certificates store.

• Cisco ISE communicates with Tenable SecurityCenter over HTTPS/SSL (port 443).

---

**Step 1** Choose **Administration > Threat Centric NAC > Third Party Vendors**.

**Step 2** Click **Add**.

**Step 3** From the **Vendor** drop-down list, choose **Tenable Security Center: VA**.

**Step 4** Enter a name for the adapter instance. For example, Tenable.

The listing page appears with a list of configured adapter instances.

**Step 5** Refresh the Vendor Instances listing page. The status for the newly added Tenable adapter should change to **Ready to Configure**.

**Step 6** Click the **Ready to Configure** link.

**Step 7** Enter the following values in the Tenable SecurityCenter configuration screen and click **Next**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tenable SecurityCenter Host</td>
<td>The hostname of the Tenable SecurityCenter.</td>
</tr>
<tr>
<td>Tenable SecurityCenter Port</td>
<td>443</td>
</tr>
<tr>
<td>Username</td>
<td>Username of the user account that has Security Manager privileges in Tenable SecurityCenter.</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the user account that has Security Manager privileges in Tenable SecurityCenter.</td>
</tr>
<tr>
<td>HTTP Proxy Host</td>
<td>If you have a proxy server configured to route all Internet traffic, enter the hostname of the proxy server.</td>
</tr>
<tr>
<td>HTTP Proxy Port</td>
<td>Enter the port number used by the proxy server.</td>
</tr>
</tbody>
</table>

**Step 8** Click **Next**.

**Step 9** Enter the following values in the Advanced Settings page. The settings in this page determine whether an on-demand scan will be triggered or the last scan results will be used for VA.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repository</td>
<td>Choose the repository that you created in Tenable SecurityCenter.</td>
</tr>
<tr>
<td>Scan Policy</td>
<td>Choose the scan policy that you have created for ISE in Tenable SecurityCenter.</td>
</tr>
</tbody>
</table>

*Settings for checking latest scan results*
### Configure Authorization Profile

The authorization profile in Cisco ISE now includes an option to scan endpoints for vulnerabilities. You can choose to run the scan periodically and also specify the time interval for these scans. After you define the authorization profile, you can apply it to an existing authorization policy rule or create a new authorization policy rule.

### Before you begin

You must have enabled the Threat Centric NAC service and configured a vendor adapter.
Configure Exception Rule to Quarantine a Vulnerable Endpoint

You can use the following Vulnerability Assessment attributes to configure an exception rule and provide limited access to vulnerable endpoints:

- Threat:Qualys-CVSS_Base_Score
- Threat:Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

These attributes are available in the Threat directory. Valid value ranges from 0 to 10.

You can choose to quarantine the endpoint, provide limited access (redirect to a different portal), or reject the request.

Vulnerability Assessment Logs

Cisco ISE provides the following logs for troubleshooting VA services.

- `vaservice.log`—Contains VA core information and is available in the node that runs the TC-NAC service.
- `varuntime.log`—Contains information about the endpoint and the VA flow; is available in the Monitoring node and the node that runs the TC-NAC service.
- `vaaggregation.log`—Contains hourly aggregation details about the endpoint vulnerability and is available in the Primary Administration Node.
Configure Smart Licensing and Smart Call Home Services

- Cisco ISE Smart Licensing, on page 637
- Smart Call Home, on page 641

Cisco ISE Smart Licensing

Cisco offers Smart Licensing, which enables you to monitor ISE software licenses and endpoint license consumption easily and efficiently with a single token registration, rather than individually importing separate licenses. Details of all Cisco products and licenses that you have purchased are maintained in a centralized database, called the Cisco Smart Software Manager (CSSM), where you can easily track which endpoint licenses are available to you, and consumption statistics.

When a smart license token is activated and registered from ISE, it monitors consumption of licenses by each endpoint session per product license. Smart Licensing notifies the administrator about license consumption by endpoint sessions from a simple table layout in ISE. Smart Licensing reports the peak usage of each enabled license to the centralized database daily. When licenses are available and not consumed, the administrator is notified of available licenses and can continue to monitor usage. When consumption exceeds the amount of licenses available, an alarm is activated and the administrator is notified through alarms and notifications.

With Smart Licensing, you can also manage the different license entitlements included through your Cisco Smart Account, such as Base, Plus, Apex, or TACACS. From ISE, you can monitor basic consumption statistics per license entitlement. From your CSSM account, you can also view additional information, statistics and notifications, as well as make changes to your account and entitlements.

Note

Cisco Smart Software Manager satellite is not supported.

ISE takes internal samples of license consumption every 30 minutes, and compliancy and consumption is updated accordingly. To view this information in the Licenses table in ISE, you need only click Refresh. At 1:00 AM every day, ISE reports peak counts daily to the CSSM server (the centralized database) based on the Yesterday's Peak Count data that is also displayed in the Licenses table, for each enabled license. ISE communicates with the CSSM server by storing a local copy of the CSSM certificate, which is automatically re-authorized during the daily synchronization, and also when the user manually refreshes the Licenses table. Typically, certificates are valid for six months. If compliancy changes when synchronized with the CSSM server, the Last Authorization column of the Licenses table updates accordingly. In addition, when entitlements...
are no longer compliant, the number of days for which they are out of compliancy appears in the Days Out of Compliancy column. Non-compliancy is also indicated in Notifications at the top of the Licensing area, and on the ISE toolbar at the **License Warning** link. In addition to notifications, you can view Alarms. For more information, see *Cisco ISE Alarms*, on page 862.

---

**Note**

TACACS licenses are authorized when ISE communicates with the CSSM server, but they are not session-based and therefore no consumption count is associated with them in the Licenses table.

---

**Figure 48: Licenses Table**

![Licenses Table](image)

---

## Activate and Register Smart Licensing in ISE

**Before you begin**

Activate Smart Licensing and then register from ISE using the token issued to you by your Cisco representative through your CSSM account.

Ensure you have the necessary ISE permissions in your Cisco Smart Software Manager (CSSM) account. For more information, see [https://software.cisco.com/](https://software.cisco.com/) or contact your Cisco representative.

If you are upgrading from ISE-PIC, then prior to activating Smart Licensing with this procedure, you must first install the ISE Upgrade license and then:

- Install the ISE Base license.

- Or, move your PIC installation to an existing ISE deployment:
  1. From the existing ISE deployment, add an additional ISE node.
  2. Enable session profiling and pxGrid services from an existing ISE Administration node.

**Note**

For more information about adding and configuring additional ISE nodes, see *Configure a Cisco ISE Node*, on page 51.

---

**Step 1**

Choose **Administration > System > Licensing** to access the **Licensing** area of ISE.

Once you have installed or upgraded your ISE box, before you activate your smart license, when you enter the **Licensing** area of ISE, traditional licensing is in use by default and appears at the top of the screen in the **Licensing Method** area:
Step 2  
Click the Cisco Smart Licensing link from the Licensing Method area to switch to Smart Licensing. The Cisco Smart Licensing area expands with connection method fields.

Step 3 From the Cisco Smart Licensing area, in the Secondary UDI field, if at least one additional ISE box is configured in your network, enter the secondary node you to be used if the Primary node is not available. Select a connection method by which to connect from your ISE box to the CSSM from the Connection Method dropdown list and click Enable. For Connection Method, choose:

a) Direct HTTPS if you have a direct connection configured to reach the Internet.

b) HTTPS Proxy if you do not have a direct connection and need to connect by proxy.

c) Transport Gateway is the recommended connection method. When you use Smart Licensing, Smart Call Home (SCH) services are automatically activated as well, enabling you to configure a Transport Gateway. To configure Transport Gateway as your connection method, first configure it from the Smart Call Home settings in the Administration work center. To do this, and for additional information about SCH and Transport Gateway, see Smart Call Home, on page 641.

Note Once you activate Smart Licensing you have a 90-day evaluation period during which time all licenses are enabled. During this time, you can explore Smart Licensing and all of the ISE features. You must continue to the next step to register for Smart Licensing with a valid token before the evaluation period expires in order to continue using ISE.

The fields in this area are dynamic. Once you have entered the connection details and click Enable, the area collapses. When you expand the area again, now called Cisco Smart Licensing Registration, you can enter smart licensing token details.
Step 4  From the **Cisco Smart Licensing Registration** area in ISE, enter the **Registration Token** you received when you purchased the smart licensing token, and click **Register**. To retrieve the token at any time, go to the ISE area of your CSSM account and click **Copy**.

You can also choose to disable any of the licenses included in your smart licensing token by removing checkmarks. When you disable the licenses, they are no longer checked for validity automatically as part of the Smart Licensing functionality.

---

**Manage Smart Licensing in ISE**

Once you have activated and registered your Smart Licensing token, you can manage license entitlements from ISE by:

- Enabling, disabling and refreshing license entitlement certificates.
- Updating Smart Licensing registration.
- Identifying compliant and non-compliant licensing issues.

**Before you begin**

Ensure you have activated and registered your Smart Licensing token. For more information, see **Activate and Register Smart Licensing in ISE**, on page 638.

---

Step 1  When you first activate Smart Licensing, all license entitlements are enabled automatically as part of the evaluation period. Once you register your token, if your CSSM account does not include certain entitlements and you did not disable them during registration, non-compliant notifications will appear in ISE. Add those entitlements to your CSSM account (contact your CSSM account representative for assistance), and then from the Licenses table, click **Refresh** to remove non-compliant notifications and continue to use the related features. Once you have refreshed authorization, log out and then log back in to ISE for the relevant non-compliancy messages to be removed.

Step 2  If the daily automatic authorization does not succeed for any reason, non-compliancy messages may appear. Click **Refresh** to re-authorize your entitlements. Once you have refreshed authorization, log out and then log back in to ISE for the relevant non-compliancy messages to be removed.

Step 3  When you first activate Smart Licensing, all license entitlements are enabled automatically as part of the evaluation period. Once you register your token, if your CSSM account does not include certain entitlements and you did not disable them during registration, you can still disable those entitlements from Smart Licensing in ISE in order to avoid unnecessary non-compliant notifications. From the Licenses table, checkmark the license entitlements that are not included in your token, and click **Disable** from the toolbar. Once you have disabled license entitlements, log out and then log back in to ISE for the relevant features to be removed from the menus and for the non-compliancy messages to be removed.

Step 4  Once you add entitlements to your account, enable those entitlements. From the Licenses table, checkmark the required disabled licenses and click **Enable** from the toolbar.

Step 5  If you initially set-up Smart Licensing with only one UDI and do not enter a Secondary UDI, you can later update your information. Click the **Cisco Smart Licensing Registration Details** link to open the area. Re-enter the token, enter the new **Secondary UDI** and click **Update**.

Step 6  The registration certificate is automatically refreshed every six months. To manually refresh your Smart Licensing certificate registration, click **Renew Registration** from the top of the Cisco Smart Licensing area.

Step 7  To remove your ISE box registration (indicated by UDIs) from your Smart Account but continue to use Smart Licensing to the end of the evaluation period, click **Deregister** from the top of the Cisco Smart Licensing area. You can do this, for example, if you need to change the UDIs you have indicated as part of the registration process. If you still have time
remaining in your evaluation period, ISE remains in Smart Licensing. If you have no time remaining in your evaluation period, a notification appears when the browser refreshes. Once you deregister, you can follow the registration process again in order to register with the same or different UDIs. For more information about activating and registering your Smart Licensing, see Activate and Register Smart Licensing in ISE, on page 638.

**Step 8** To remove your ISE box registration (indicated by UDIs) from your Smart Account entirely and to revert to traditional licensing, click **Disable** from the top of the Cisco Smart Licensing area. You can do this, for example, if you need to change the UDIs you have indicated as part of the registration process. Once you disable, you can follow the registration process again in order to activate and register with the same or different UDIs. For more information about activating and registering your Smart Licensing, see Activate and Register Smart Licensing in ISE, on page 638.

---

**Smart Call Home**

The Smart Call Home (SCH) feature monitors Cisco ISE devices in your network and notifies you via e-mail about the critical events if configured on Smart Call Home portal. It also provides real-time alerts with remediation advice for issues that are detected. SCH monitors and sends event notifications for Environment issues.

When you activate Smart Licensing from Cisco ISE, the SCH capabilities are enabled by default. Otherwise, to enable SCH, you must register Cisco ISE for the SCH service. See Register for Smart Call Home Service, on page 642 for information on how to enable the SCH feature. After you activate Smart Licensing or register for the SCH service, you can choose to do one of the following:

- Enable only Anonymous Reporting. The Anonymous Reporting feature of SCH provides minimal health information about the Cisco ISE devices in your network.
- Enable the full set of features offered by SCH.

For more information on enabling the SCH capabilities, see Register for Smart Call Home Service, on page 642.

Cisco ISE provides support for Transport Gateway. If your organization's security policy does not allow communication between the ISE servers in your network and the SCH servers, you can use an optional Transport Gateway to act as a proxy for SCH communication. The Transport Gateway software can be downloaded from Cisco.com and can be installed and maintained on a Linux server. Refer to the Smart Call Home Deployment Guide for information on how to deploy the Transport Gateway software on an RHEL server.

---

**Smart Call Home Profiles**

Smart Call Home profiles determine the types of events that are monitored on your device. Cisco ISE includes the following default profiles:

- ciscotac-1 - Used for anonymous reporting
- isesch-1 - Used for Smart Call Home functionality

You cannot edit the default profile that is used for anonymous reporting (ciscotac-1).
Anonymous Reporting

Cisco ISE securely collects non-sensitive information about your deployment, network access devices, profiler, and other services that you are using. This data is collected to better understand Cisco ISE usage and to improve the product and the various services that it offers.

By default, anonymous reporting is enabled. If you want to disable anonymous reporting, you can do so from the ISE Admin Portal (Administration > System > Settings > Smart Call Home).

Register for Smart Call Home Service

---

**Note**

If you have activated Smart Licensing from Cisco ISE, you don't have to register for the Smart Call Home (SCH) service. With Smart Licensing, the SCH capabilities are enabled by default. The Registration Status in the Smart Call Home page would be Active. You can choose to enable only Anonymous Reporting or enable the full set of features offered by SCH.

To enable SCH services without Smart Licensing, you must first register Cisco ISE for the SCH service. You can only do so from a standalone node or a Primary Administration Node.

---

**Step 1** Choose Administration > System > Settings > Smart Call Home.

**Step 2** Choose one of the following:

- Turn on full SCH capability
- Keep the default SCH telemetry settings and send only anonymous data
- Disable everything

**Step 3** (Only if you choose the Turn on full SCH Capability option) Enter your e-mail address in the Registration Status area.

**Step 4** (Optional) Check the Transport Gateway check box and enter the Transport Gateway URL.

**Step 5** Click Save.

You will receive an e-mail with the activation link, if you have chosen to turn on full SCH capability. Click the activation link and follow the instructions provided to complete the registration.
Cisco ISE Profiling Service

The profiling service in Cisco Identity Services Engine (ISE) identifies the devices that connect to your network and their location. The endpoints are profiled based on the endpoint profiling policies configured in Cisco ISE. Cisco ISE then grants permission to the endpoints to access the resources in your network based on the result of the policy evaluation.
The profiling service:

- Facilitates an efficient and effective deployment and ongoing management of authentication by using IEEE standard 802.1X port-based authentication access control, MAC Authentication Bypass (MAB) authentication, and Network Admission Control (NAC) for any enterprise network of varying scale and complexity.
- Identifies, locates, and determines the capabilities of all of the attached network endpoints regardless of endpoint types.
- Protects against inadvertently denying access to some endpoints.

ISE Community Resource
ISE Endpoint Profiles
How To: ISE Profiling Design Guide

Profiler Work Center

The Profiler Work Center menu (Work Centers > Profiler) contains all the profiler pages, which acts as a single start point for ISE administrators. The Profiler Work Center menu contains the following options: Overview, Ext ID Stores, Network Devices, Endpoint Classification, Node Config, Feeds, Manual Scans, Policy Elements, Profiling Policies, Authorization Policy, Troubleshoot, Reports, Settings, and Dictionaries.

Profiler Dashboard

The Profiler dashboard (Work Centers > Profiler > Endpoint Classification) is a centralized monitoring tool for the profiles, endpoints, and assets in your network. The dashboard represents data in both graphical and table formats. The Profiles dashlet displays the logical and endpoint profiles that are currently active in the network. The Endpoints dashlet displays the identity group, PSNs, OS types of the endpoints that connect to your network. The Assets dashlet displays flows such as Guest, BYOD, and Corporate. The table displays the various endpoints that are connected and you can also add new endpoints.

Endpoint Inventory Using Profiling Service

You can use the profiling service to discover, locate, and determine the capabilities of all the endpoints connected to your network. You can ensure and maintain appropriate access of endpoints to the enterprise network, regardless of their device types.

The profiling service collects attributes of endpoints from the network devices and the network, classifies endpoints into a specific group according to their profiles, and stores endpoints with their matched profiles in the Cisco ISE database. All the attributes that are handled by the profiling service need to be defined in the profiler dictionaries.

The profiling service identifies each endpoint on your network, and groups those endpoints according to their profiles to an existing endpoint identity group in the system, or to a new group that you can create in the system. By grouping endpoints, and applying endpoint profiling policies to the endpoint identity group, you can determine the mapping of endpoints to the corresponding endpoint profiling policies.
Cisco ISE Profiler Queue Limit Configuration

Cisco ISE profiler collects a significant amount of endpoint data from the network in a short period of time. It causes Java Virtual Machine (JVM) memory utilization to go up due to accumulated backlog when some of the slower Cisco ISE components process the data generated by the profiler, which results in performance degradation and stability issues.

To ensure that the profiler does not increase the JVM memory utilization and prevent JVM to go out of memory and restart, limits are applied to the following internal components of the profiler:

- **Endpoint Cache**—Internal cache is limited in size that has to be purged periodically (based on least recently used strategy) when the size exceeds the limit.
- **Forwarder**—The main ingress queue of endpoint information collected by the profiler.
- **EventHandler**—An internal queue that disconnects a fast component, which feeds data to a slower processing component (typically related to a database query).

**Endpoint Cache**

- maxEndPointsInLocalDb = 100000 (endpoint objects in cache)
- endpointsPurgeIntervalSec = 300 (endpoint cache purge thread interval in seconds)
- numberOfProfilingThreads = 8 (number of threads)

The limit is applicable to all profiler internal event handlers. A monitoring alarm is triggered when queue size limit is reached.

**Cisco ISE Profiler Queue Size Limits**

- forwarderQueueSize = 5000 (endpoint collection events)
- eventHandlerQueueSize = 10000 (events)

**Event Handlers**

- NetworkDeviceEventHandler—For network device events, in addition to filtering duplicate Network Access Device (NAD) IP addresses, which are already cached.
- ARPCacheEventHandler—For ARP Cache events.

Configure Profiling Service in Cisco ISE Nodes

You can configure the profiling service that provides you a contextual inventory of all the endpoints that are using your network resources in any Cisco ISE-enabled network.

You can configure the profiling service to run on a single Cisco ISE node that assumes all Administration, Monitoring, and Policy Service personas by default.

In a distributed deployment, the profiling service runs only on Cisco ISE nodes that assume the Policy Service persona and does not run on other Cisco ISE nodes that assume the Administration and Monitoring personas.
Step 1  Choose Administration > System > Deployment.

Step 2  Choose a Cisco ISE node that assumes the Policy Service persona.

Step 3  Click Edit in the Deployment Nodes page.

Step 4  On the General Settings tab, check the Policy Service check box. If the Policy Service check box is unchecked, both the session services and the profiling service check boxes are disabled.

Step 5  Perform the following tasks:
   a) Check the Enable Session Services check box to run the Network Access, Posture, Guest, and Client Provisioning session services.
   b) Check the Enable Profiling Services check box to run the profiling service.
   c) Check the Enable Device Admin Service check box to run the device administration service to control and audit an enterprise's network devices.

Step 6  Click Save to save the node configuration.

Network Probes Used by Profiling Service

Network probe is a method used to collect an attribute or a set of attributes from an endpoint on your network. The probe allows you to create or update endpoints with their matched profile in the Cisco ISE database.

Cisco ISE can profile devices using a number of network probes that analyze the behavior of devices on the network and determine the type of the device. Network probes help you to gain more network visibility.

IP Address and MAC Address Binding

You can create or update endpoints only by using their MAC addresses in an enterprise network. If you do not find an entry in the ARP cache, then you can create or update endpoints by using the L2 MAC address of an HTTP packet and the IN_SRC_MAC of a NetFlow packet in Cisco ISE. The profiling service is dependent on L2 adjacency when endpoints are only a hop away. When endpoints are L2 adjacent, the IP addresses and MAC addresses of endpoints are already mapped, and there is no need for IP-MAC cache mapping. If endpoints are not L2 adjacent and are multiple hops away, mapping may not be reliable. Some of the known attributes of NetFlow packets that you collect include PROTOCOL, L4_SRC_PORT, IPV4_SRC_ADDR, L4_DST_PORT, IPV4_DST_ADDR, IN_SRC_MAC, OUT_DST_MAC, IN_SRC_MAC, and OUT_SRC_MAC. When endpoints are not L2 adjacent and are multiple L3 hops away, the IN_SRC_MAC attributes carry only the MAC addresses of L3 network devices. When the HTTP probe is enabled in Cisco ISE, you can create endpoints only by using the MAC addresses of HTTP packets, because the HTTP request messages do not carry IP addresses and MAC addresses of endpoints in the payload data. Cisco ISE implements an ARP cache in the profiling service, so that you can reliably map the IP addresses and the MAC addresses of endpoints. For the ARP cache to function, you must enable either the DHCP probe or the RADIUS probe. The DHCP and RADIUS probes carry the IP addresses and the MAC addresses of endpoints in the payload data. The dhcp-requested address attribute in the DHCP probe and the Framed-IP-address attribute in the RADIUS probe carry the IP addresses of endpoints, along with their MAC addresses, which can be mapped and stored in the ARP cache.
NetFlow Probe

Cisco ISE profiler implements Cisco IOS NetFlow Version 9. We recommend using NetFlow Version 9, which has additional functionality needed to enhance the profiler to support the Cisco ISE profiling service. You can collect NetFlow Version 9 attributes from the NetFlow-enabled network access devices to create an endpoint, or update an existing endpoint in the Cisco ISE database. You can configure NetFlow Version 9 to attach the source and destination MAC addresses of endpoints and update them. You can also create a dictionary of NetFlow attributes to support NetFlow-based profiling.

For more information on the NetFlow Version 9 Record Format, see Table 6, “NetFlow Version 9 Field Type Definitions” of the NetFlow Version 9 Flow-Record Format document.

In addition, Cisco ISE supports NetFlow versions earlier than Version 5. If you use NetFlow Version 5 in your network, then you can use Version 5 only on the primary network access device (NAD) at the access layer because it will not work anywhere else.

Cisco IOS NetFlow Version 5 packets do not contain MAC addresses of endpoints. The attributes that are collected from NetFlow Version 5 cannot be directly added to the Cisco ISE database. You can discover endpoints by using their IP addresses, and append the NetFlow Version 5 attributes to endpoints, which can be done by combining IP addresses of the network access devices and IP addresses obtained from the NetFlow Version 5 attributes. However, these endpoints must have been previously discovered with the RADIUS or SNMP probe.

The MAC address is not a part of IP flows in earlier versions of NetFlow Version 5, which requires you to profile endpoints with their IP addresses by correlating the attributes information collected from the network access devices in the endpoints cache.

For more information on the NetFlow Version 5 Record Format, see Table 2, “Cisco IOS NetFlow Flow Record and Export Format Content Information” of the NetFlow Services Solutions Guide.

DHCP Probe

The Dynamic Host Configuration Protocol probe in your Cisco ISE deployment, when enabled, allows the Cisco ISE profiling service to reprofile endpoints based only on new requests of INIT-REBOOT, and SELECTING message types. Though other DHCP message types such as RENEWING and REBINDING are processed, they are not used for profiling endpoints. Any attribute parsed out of DHCP packets is mapped to endpoint attributes.

DHCPREQUEST Message Generated During INIT-REBOOT State

If the DHCP client checks to verify a previously allocated and cached configuration, then the client must not fill in the Server identifier (server-ip) option. Instead it should fill in the Requested IP address (requested-ip) option with the previously assigned IP address, and fill in the Client IP Address (ciaddr) field with zero in its DHCPREQUEST message. The DHCP server will then send a DHCPNAK message to the client if the Requested IP address is incorrect or the client is located in the wrong network.

DHCPREQUEST Message Generated During SELECTING State

The DHCP client inserts the IP address of the selected DHCP server in the Server identifier (server-ip) option, fills in the Requested IP address (requested-ip) option with the value of the Your IP Address (yiaddr) field from the chosen DHCPOFFER by the client, and fills in the “ciaddr” field with zero.
Wireless LAN Controller Configuration in DHCP Bridging Mode

We recommend that you configure wireless LAN controllers (WLCs) in Dynamic Host Configuration Protocol (DHCP) bridging mode, where you can forward all the DHCP packets from the wireless clients to Cisco ISE. You must uncheck the Enable DHCP Proxy check box available in the WLC web interface: Controller > Advanced > DHCP Master Controller Mode > DHCP Parameters. You must also ensure that the DHCP IP helper command points to the Cisco ISE Policy Service node.

DHCP SPAN Probe

The DHCP Switched Port Analyzer (SPAN) probe, when initialized in a Cisco ISE node, listens to network traffic, which are coming from network access devices on a specific interface. You need to configure network access devices to forward DHCP SPAN packets to the Cisco ISE profiler from the DHCP servers. The profiler receives these DHCP SPAN packets and parses them to capture the attributes of an endpoint, which can be used for profiling endpoints.

For example,

```
switch(config)# monitor session 1 source interface Gi1/0/4
switch(config)# monitor session 1 destination interface Gi1/0/2
```

HTTP Probe

In HTTP probe, the identification string is transmitted in an HTTP request-header field User-Agent, which is an attribute that can be used to create a profiling condition of IP type, and to check the web browser information. The profiler captures the web browser information from the User-Agent attribute along with other HTTP attributes from the request messages, and adds them to the list of endpoint attributes.

Cisco ISE listens to communication from the web browsers on both port 80 and port 8080. Cisco ISE provides many default profiles, which are built in to the system to identify endpoints based on the User-Agent attribute.

HTTP SPAN Probe

The HTTP probe in your Cisco ISE deployment, when enabled with the Switched Port Analyzer (SPAN) probe, allows the profiler to capture HTTP packets from the specified interfaces. You can use the SPAN capability on port 80, where the Cisco ISE server listens to communication from the web browsers.

HTTP SPAN collects HTTP attributes of an HTTP request-header message along with the IP addresses in the IP header (L3 header), which can be associated to an endpoint based on the MAC address of an endpoint in the L2 header. This information is useful for identifying different mobile and portable IP-enabled devices.

---

Table 42: DHCP Client Messages from Different States

<table>
<thead>
<tr>
<th>—</th>
<th>INIT-REBOOT</th>
<th>SELECTING</th>
<th>RENEWING</th>
<th>REBINDING</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast/unicast</td>
<td>broadcast</td>
<td>broadcast</td>
<td>unicast</td>
<td>broadcast</td>
</tr>
<tr>
<td>server-ip</td>
<td>MUST NOT</td>
<td>MUST</td>
<td>MUST NOT</td>
<td>MUST NOT</td>
</tr>
<tr>
<td>requested-ip</td>
<td>MUST</td>
<td>MUST</td>
<td>MUST NOT</td>
<td>MUST NOT</td>
</tr>
<tr>
<td>ciaddr</td>
<td>zero</td>
<td>zero</td>
<td>IP address</td>
<td>IP address</td>
</tr>
</tbody>
</table>
such as Apple devices, and computers with different operating systems. Identifying different mobile and portable IP-enabled devices is made more reliable because the Cisco ISE server redirects captures during a guest login or client provisioning download. This allows the profiler to collect the User-Agent attribute and other HTTP attributes, from the request messages and then identify devices such as Apple devices.

Unable to Collect HTTP Attributes in Cisco ISE Running on VMware

If you deploy Cisco ISE on an ESX server (VMware), the Cisco ISE profiler collects the Dynamic Host Configuration Protocol traffic but does not collect the HTTP traffic due to configuration issues on the vSphere client. To collect HTTP traffic on a VMware setup, configure the security settings by changing the Promiscuous Mode to Accept (by default) of the virtual switch that you create for the Cisco ISE profiler. When the Switched Port Analyzer (SPAN) probe for DHCP and HTTP is enabled, Cisco ISE profiler collects both the DHCP and HTTP traffic.

RADIUS Probe

You can configure Cisco ISE for authentication with RADIUS, where you can define a shared secret that you can use in client-server transactions. With the RADIUS request and response messages that are received from the RADIUS servers, the profiler can collect RADIUS attributes, which can be used for profiling endpoints. Cisco ISE can function as a RADIUS server, and a RADIUS proxy client to other RADIUS servers. When it acts as a proxy client, it uses external RADIUS servers to process RADIUS requests and response messages.

Network Scan (NMAP) Probe

About the NMAP Probe

Cisco ISE enables you to detect devices in a subnet by using the NMAP security scanner. You enable the NMAP probe on the Policy Service node that is enabled to run the profiling service. You use the results from that probe in an endpoint profiling policy.

Each NMAP manual subnet scan has a unique numeric ID that is used to update an endpoint source information with that scan ID. Upon detection of endpoints, the endpoint source information can also be updated to indicate that it is discovered by the Network Scan probe.

The NMAP manual subnet scan is useful for detecting devices such as printers with a static IP address assigned to them that are connected constantly to the Cisco ISE network, and therefore these devices cannot be discovered by other probes.

NMAP Scan Limitations

Scanning a subnet is highly resource intensive. Scanning a subnet is a lengthy process that depends on the size and density of the subnet. Number of active scans is always restricted to one scan, which means that you can scan only a single subnet at a time. You can cancel a subnet scan at any time while the subnet scan is in progress. You can use the Click to see latest scan results link to view the most recent network scan results that are stored in Work Centers > Profiler > Manual Scans > Manual NMAP Scan Results.

Manual NMAP Scan

The following NMAP command scans a subnet and sends the output to nmapSubnet.log:

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log --append-output -oX = <subnet>
```
Table 43: NMAP Commands for a Manual Subnet Scan

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-O</td>
<td>Enables OS detection</td>
</tr>
<tr>
<td>-sU</td>
<td>UDP scan</td>
</tr>
<tr>
<td>-p &lt;port ranges&gt;</td>
<td>Scans only specified ports. For example, U:161, 162</td>
</tr>
<tr>
<td>oN</td>
<td>Normal output</td>
</tr>
<tr>
<td>oX</td>
<td>XML output</td>
</tr>
</tbody>
</table>

SNMP Read Only Community Strings for NMAP Manual Subnet Scan

The NMAP manual subnet scan is augmented with an SNMP Query whenever the scan discovers that UDP port 161 is open on an endpoint that results in more attributes being collected. During the NMAP manual subnet scan, the Network Scan probe detects whether SNMP port 161 is open on the device. If the port is open, an SNMP Query is triggered with a default community string (public) with SNMP version 2c. If the device supports SNMP and the default Read Only community string is set to public, you can obtain the MAC address of the device from the MIB value “iPhysAddress”. In addition, you can configure additional SNMP Read Only community strings separated by a comma for the NMAP manual network scan in the Profiler Configuration page. You can also specify new Read Only community strings for an SNMP MIB walk with SNMP versions 1 and 2c in the following location: Administration > System > Settings > Profiling.

Manual NMAP Scan Results

The most recent network scan results are stored in Work Centers > Profiler > Manual Scans > Manual NMAP Scan Results. The Manaul NMAP Scan Results page displays only the most recent endpoints that are detected, along with their associated endpoint profiles, their MAC addresses, and their static assignment status as the result of a manual network scan you perform on any subnet. This page allows you to edit points that are detected from the endpoint subnet for better classification, if required.

Cisco ISE allows you to perform the manual network scan from the Policy Service nodes that are enabled to run the profiling service. You must choose the Policy Service node from the primary Administration ISE node user interface in your deployment to run the manual network scan from the Policy Service node. During the manual network scan on any subnet, the Network Scan probe detects endpoints on the specified subnet, their operating systems, and check UDP ports 161 and 162 for an SNMP service.

Additional Information

Given below is additional information related to the manual NMAP scan results:

- To detect unknown endpoints, NMAP should be able to learn the IP/MAC binding via NMAP or a supporting SNMP scan.
- ISE learns IP/MAC binding of known endpoints via Radius authentication or DHCP profiling.
- The IP/MAC bindings are not replicated across PSN nodes in a deployment. Therefore, you must trigger the manual scan from the PSN, which has the IP/MAC binding in its local database (for example, the PSN against which a mac address was last authenticated with).
- The NMAP scan results do not display any information related to an endpoint that NMAP had previously scanned, manually or automatically.
DNS Probe

The Domain Name Service (DNS) probe in your Cisco ISE deployment allows the profiler to lookup an endpoint and get the fully qualified domain name (FQDN). After an endpoint is detected in your Cisco ISE-enabled network, a list of endpoint attributes is collected from the NetFlow, DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP probes.

When you deploy Cisco ISE in a standalone or in a distributed environment for the first time, you are prompted to run the setup utility to configure the Cisco ISE appliance. When you run the setup utility, you will configure the Domain Name System (DNS) domain and the primary nameserver (primary DNS server), where you can configure one or more nameservers during setup. You can also change or add DNS nameservers later after deploying Cisco ISE using the CLI commands.

DNS FQDN Lookup

Before a DNS lookup can be performed, one of the following probes must be started along with the DNS probe: DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP. This allows the DNS probe in the profiler to do a reverse DNS lookup (FQDN lookup) against specified name servers that you define in your Cisco ISE deployment. A new attribute is added to the attribute list for an endpoint, which can be used for an endpoint profiling policy evaluation. The FQDN is the new attribute that exists in the system IP dictionary. You can create an endpoint profiling condition to validate the FQDN attribute and its value for profiling. The following are the specific endpoint attributes that are required for a DNS lookup and the probe that collects these attributes:

• The dhcp-requested-address attribute—An attribute collected by the DHCP and DHCP SPAN probes.
• The SourceIP attribute—An attribute collected by the HTTP probe
• The Framed-IP-Address attribute—An attribute collected by the RADIUS probe
• The cdpcacheAddress attribute—An attribute collected by the SNMP probe

Configure Call Station ID Type in the WLC Web Interface

You can use the WLC web interface to configure Call Station ID Type information. You can go to the Security tab of the WLC web interface to configure the calling station ID in the RADIUS Authentication Servers page. The MAC Delimiter field is set to Colon by default in the WLC user interface.

For more information on how to configure in the WLC web interface, see Chapter 6, “Configuring Security Solutions” in the Cisco Wireless LAN Controller Configuration Guide, Release 7.2.

For more information on how to configure in the WLC CLI using the config radius callStationIdType command, see Chapter 2, “Controller Commands” in the Cisco Wireless LAN Controller Command Reference Guide, Release 7.2.

Step 1 Log in to your Wireless LAN Controller user interface.
Step 2 Click Security.
Step 3 Expand AAA, and then choose RADIUS > Authentication.
Step 4 Choose System MAC Address from the Call Station ID Type drop-down list.
Step 5 Check the AES Key Wrap check box when you run Cisco ISE in FIPS mode.
Step 6  Choose **Colon** from the MAC Delimeter drop-down list.

---

**SNMP Query Probe**

In addition to configuring the SNMP Query probe in the Edit Node page, you must configure other Simple Management Protocol settings in the following location: **Administration > Network Resources > Network Devices**.

You can configure SNMP settings in the new network access devices (NADs) in the Network Devices list page. The polling interval that you specify in the SNMP query probe or in the SNMP settings in the network access devices query NADs at regular intervals.

You can turn on and turn off SNMP querying for specific NADs based on the following configurations:

- SNMP query on Link up and New MAC notification turned on or turned off
- SNMP query on Link up and New MAC notification turned on or turned off for Cisco Discovery Protocol information
- SNMP query timer for once an hour for each switch by default

For an iDevice, and other mobile devices that do not support SNMP, the MAC address can be discovered by the ARP table, which can be queried from the network access device by an SNMP Query probe.

**Cisco Discovery Protocol Support with SNMP Query**

When you configure SNMP settings on the network devices, you must ensure that the Cisco Discovery Protocol is enabled (by default) on all the ports of the network devices. If you disable the Cisco Discovery Protocol on any of the ports on the network devices, then you may not be able to profile properly because you will miss the Cisco Discovery Protocol information of all the connected endpoints. You can enable the Cisco Discovery Protocol globally by using the `cdprun` command on a network device, and enable the Cisco Discovery Protocol by using the `cdpenable` command on any interface of the network access device. To disable the Cisco Discovery Protocol on the network device and on the interface, use the `no` keyword at the beginning of the commands.

**Link Layer Discovery Protocol Support with SNMP Query**

The Cisco ISE profiler uses an SNMP Query to collect LLDP attributes. You can also collect LLDP attributes from a Cisco IOS sensor, which is embedded in the network device, by using the RADIUS probe. See the default LLDP configuration settings that you can use to configure LLDP global configuration and LLDP interface configuration commands on the network access devices.

**Table 44: Default LLDP Configuration**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>LLDP global state</td>
<td>Disabled</td>
</tr>
<tr>
<td>LLDP holdtime (before discarding)</td>
<td>120 seconds</td>
</tr>
<tr>
<td>LLDP timer (packet update frequency)</td>
<td>30 seconds</td>
</tr>
<tr>
<td>LLDP reinitialization delay</td>
<td>2 seconds</td>
</tr>
</tbody>
</table>
Enable and Configure Cisco ISE Services

CDP and LLDP Capability Codes Displayed in a Single Character

The Attribute List of an endpoint displays a single character value for the lldpCacheCapabilities and lldpCapabilitiesMapSupported attributes. The values are the Capability Codes that are displayed for the network access device that runs CDP and LLDP.

Example 1

```
lldpCacheCapabilities S
lldpCapabilitiesMapSupported S
```

Example 2

```
lldpCacheCapabilities B;T
lldpCapabilitiesMapSupported B;T
```

Example 3

```
Switch#show cdp neighbors
Capability Codes:
R - Router, T - Trans Bridge, B - Source Route Bridge, S - Switch, H - Host, I - IGMP,
r - Repeater, P - Phone, D - Remote, C - CVTA, M - Two-port Mac Relay
...
Switch#
Switch#show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other
...
Switch#
```

SNMP Trap Probe

The SNMP Trap receives information from the specific network access devices that support MAC notification, linkup, linkdown, and informs. The SNMP Trap probe receives information from the specific network access devices when ports come up or go down and endpoints disconnect from or connect to your network, which results in the information received that is not sufficient to create endpoints in Cisco ISE.
For SNMP Trap to be fully functional and create endpoints, you must enable SNMP Query so that the SNMP Query probe triggers a poll event on the particular port of the network access device when a trap is received. To make this feature fully functional you should configure the network access device and SNMP Trap.

Cisco ISE does not support SNMP Traps that are received from the Wireless LAN Controllers (WLCs) and Access Points (APs).

**Active Directory Probe**

The AD probe:

- Improves the fidelity of OS information for Windows endpoints. Microsoft AD tracks detailed OS information for AD-joined computers including version and service pack levels. The AD probe retrieves this information directly using the AD Runtime connector to provide a highly reliable source of client OS information.

- Helps distinguish between corporate and non-corporate assets. A basic but important attribute available to the AD probe is whether an endpoint exists in AD. This information can be used to classify an endpoint contained in the AD as a managed device or corporate asset.

You can enable the AD probe under the Administration > System > Deployment > Profiling Configuration page. When this probe is enabled, ISE fetches the AD attributes for a new endpoint as soon as it receives a hostname. The hostname is typically learned from the DHCP or DNS probes. Once successfully retrieved, ISE does not attempt to query AD again for the same endpoint until a the rescan timer expires. This is to limit the load on AD for attribute queries. The rescan timer is configurable in the Days Before Rescan field (Administration > System > Deployment > Profiling Configuration > Active Directory). If there is additional profiling activity on the endpoint, the AD is queried again.

The following AD probe attributes can be matched in the Policy > Policy Elements > Profiling using the ACTIVEDIRECTORY condition. AD attributes collected using the AD Probe appear with the prefix “AD” in the endpoint details on the Context Visibility > Endpoints page.

- AD-Host-Exists
- AD-Join-Point
- AD-Operating-System
- AD-OS-Version
- AD-Service-Pack

**Configure Probes per Cisco ISE Node**

You can configure one or more probes on the Profiling Configuration tab per Cisco ISE node in your deployment that assumes the Policy Service persona, which could be:

- A standalone node—If you have deployed Cisco ISE on a single node that assumes all Administration, Monitoring, and Policy Service personas by default.
Before you begin

You can configure the probes per Cisco ISE node only from the Administration node, which is unavailable on the secondary Administration node in a distributed deployment.

---

**Step 1** Choose **Administration > System > Deployment**.

**Step 2** Choose a Cisco ISE node that assumes the Policy Service persona.

**Step 3** Click **Edit** in the Deployment Nodes page.

**Step 4** On the **General Settings** tab, check the **Policy Service** check box. If the Policy Service check box is unchecked, both the session services and the profiling service check boxes are disabled.

**Step 5** Check the **Enable Profiling Services** check box.

**Step 6** Click the **Profiling Configuration** tab.

**Step 7** Configure the values for each probe.

**Step 8** Click **Save** to save the probe configuration.

---

**Setup CoA, SNMP RO Community, and Endpoint Attribute Filter**

Cisco ISE allows a global configuration to issue a Change of Authorization (CoA) in the Profiler Configuration page that enables the profiling service with more control over endpoints that are already authenticated.

In addition, you can configure additional SNMP Read Only community strings separated by a comma for the NMAP manual network scan in the Profiler Configuration page. The SNMP RO community strings are used in the same order as they appear in the Current custom SNMP community strings field.

You can also configure endpoint attribute filtering in the Profiler Configuration page.

---

**Step 1** Choose **Administration > System > Settings > Profiling**.

**Step 2** Choose one of the following settings to configure the CoA type:

- **No CoA** (default)—You can use this option to disable the global configuration of CoA. This setting overrides any configured CoA per endpoint profiling policy.

- **Port Bounce**—You can use this option, if the switch port exists with only one session. If the port exists with multiple sessions, then use the Reauth option.

- **Reauth**—You can use this option to enforce reauthentication of an already authenticated endpoint when it is profiled.

If you have multiple active sessions on a single port, the profiling service issues a CoA with the Reauth option even though you have configured CoA with the Port Bounce option. This function avoids disconnecting other sessions, a situation that might occur with the Port Bounce option.
Global Configuration of Change of Authorization for Authenticated Endpoints

You can use the global configuration option to disable change of authorization (CoA) by using the default No CoA option or enable CoA by using port bounce and reauthentication options. If you have configured Port Bounce for CoA in Cisco ISE, the profiling service may still issue other CoAs as described in the “CoA Exemptions” section.

You can use the RADIUS probe or the Monitoring persona REST API to authenticate the endpoints. You can enable the RADIUS probe, which allows faster performance. If you have enabled CoA, then we recommend that you enable the RADIUS probe in conjunction with your CoA configuration in the Cisco ISE application for faster performance. The profiling service can then issue an appropriate CoA for endpoints by using the RADIUS attributes that are collected.

If you have disabled the RADIUS probe in the Cisco ISE application, then you can rely on the Monitoring persona REST API to issue CoAs. This allows the profiling service to support a wider range of endpoints. In a distributed deployment, your network must have at least one Cisco ISE node that assumes the Monitoring persona to rely on the Monitoring persona REST API to issue a CoA.

Cisco ISE arbitrarily will designate either the primary or secondary Monitoring node as the default destination for REST queries in your distributed deployment, because both the primary and secondary Monitoring nodes have identical session directory information.

Use Cases for Issuing Change of Authorization

The profiling service issues the change of authorization in the following cases:

- **Endpoint deleted**—When an endpoint is deleted from the Endpoints page and the endpoint is disconnected or removed from the network.

- **An exception action is configured**—If you have an exception action configured per profile that leads to an unusual or an unacceptable event from that endpoint. The profiling service moves the endpoint to the corresponding static profile by issuing a CoA.

- **An endpoint is profiled for the first time**—When an endpoint is not statically assigned and profiled for the first time; for example, the profile changes from an unknown to a known profile.
  - An endpoint identity group has changed—When an endpoint is added or removed from an endpoint identity group that is used by an authorization policy.

The profiling service issues a CoA when there is any change in an endpoint identity group, and the endpoint identity group is used in the authorization policy for the following:

- The endpoint identity group changes for endpoints when they are dynamically profiled
- The endpoint identity group changes when the static assignment flag is set to true for a dynamic endpoint
An endpoint profiling policy has changed and the policy is used in an authorization policy—When an endpoint profiling policy changes, and the policy is included in a logical profile that is used in an authorization policy. The endpoint profiling policy may change due to the profiling policy match or when an endpoint is statically assigned to an endpoint profiling policy, which is associated to a logical profile. In both the cases, the profiling service issues a CoA, only when the endpoint profiling policy is used in an authorization policy.

**Exemptions for Issuing a Change of Authorization**

The profiling service does not issue a CoA when there is a change in an endpoint identity group and the static assignment is already true.

Cisco ISE does not issue a CoA for the following reasons:

- **An Endpoint disconnected from the network**—When an endpoint disconnected from your network is discovered.
- **Authenticated wired (Extensible Authentication Protocol) EAP-capable endpoint**—When an authenticated wired EAP-capable endpoint is discovered.
- **Multiple active sessions per port**—When you have multiple active sessions on a single port, the profiling service issues a CoA with the Reauth option even though you have configured CoA with the Port Bounce option.
- **Packet-of-Disconnect CoA (Terminate Session) when a wireless endpoint is detected**—If an endpoint is discovered as wireless, then a Packet-of-Disconnect CoA (Terminate-Session) is issued instead of the Port Bounce CoA. The benefit of this change is to support the Wireless LAN Controller (WLC) CoA.
- **An Endpoint Created through Guest Device Registration flow**—When endpoints are created through device registration for the guests. Even though CoA is enabled globally in Cisco ISE, the profiling service does not issue a CoA so that the device registration flow is not affected. In particular, the PortBounce CoA global configuration breaks the flow of the connecting endpoint.
- **Global No CoA Setting overrides Policy CoA**—Global No CoA overrides all configuration settings in endpoint profiling policies as there is no CoA issued in Cisco ISE irrespective of CoA configured per endpoint profiling policy.

**Note**

No CoA and Reauth CoA configurations are not affected, and the profiler service applies the same CoA configuration for wired and wireless endpoints.
Change of Authorization Issued for Each Type of CoA Configuration

Table 45: Change of Authorization Issued for Each Type of CoA Configuration

<table>
<thead>
<tr>
<th>Scenarios</th>
<th>No CoA Configuration</th>
<th>Port Bounce Configuration</th>
<th>Reauth Configuration</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global CoA configuration in Cisco ISE (typical configuration)</td>
<td>No CoA</td>
<td>Port Bounce</td>
<td>Reauthentication</td>
<td>—</td>
</tr>
<tr>
<td>An endpoint is disconnected on your network</td>
<td>No CoA</td>
<td>No CoA</td>
<td>No CoA</td>
<td>Change of authorization is determined by the RADIUS attribute Acct-Status -Type value Stop.</td>
</tr>
<tr>
<td>Wired with multiple active sessions on the same switch port</td>
<td>No CoA</td>
<td>Reauthentication</td>
<td>Reauthentication</td>
<td>Reauthentication avoids disconnecting other sessions.</td>
</tr>
<tr>
<td>Wireless endpoint</td>
<td>No CoA</td>
<td>Packet-of-Disconnect CoA (Terminate Session)</td>
<td>Reauthentication</td>
<td>Support to Wireless LAN Controller.</td>
</tr>
<tr>
<td>Incomplete CoA data</td>
<td>No CoA</td>
<td>No CoA</td>
<td>No CoA</td>
<td>Due to missing RADIUS attributes.</td>
</tr>
</tbody>
</table>

Attribute Filters for ISE Database Persistence and Performance

Cisco ISE implements filters for Dynamic Host Configuration Protocol (both DHCP Helper and DHCP SPAN), HTTP, RADIUS, and Simple Network Management Protocol probes except for the NetFlow probe to address performance degradation. Each probe filter contains the list of attributes that are temporal and irrelevant for endpoint profiling and removes those attributes from the attributes collected by the probes.

The isebootstrap log (isebootstrap-yyyymmdd-xxxxxx.log) contains messages that handles the creation of dictionaries and with filtering of attributes from the dictionaries. You can also configure to log a debug message when endpoints go through the filtering phase to indicate that filtering has occurred.

The Cisco ISE profiler invokes the following endpoint attribute filters:

- A DHCP filter for both the DHCP Helper and DHCP SPAN contains all the attributes that are not necessary and they are removed after parsing DHCP packets. The attributes after filtering are merged with existing attributes in the endpoint cache for an endpoint.

- An HTTP filter is used for filtering attributes from HTTP packets, where there is no significant change in the set of attributes after filtering.

- A RADIUS filter is used once the syslog parsing is complete and endpoint attributes are merged into the endpoint cache for profiling.
- SNMP filter for SNMP Query includes separate CDP and LLDP filters, which are all used for SNMP-Query probe.

Global Setting to Filter Endpoint Attributes with Whitelist

You can reduce the number of persistence events and replication events by reducing the number of endpoint attributes that do not change frequently at the collection point. Enabling the EndPoint Attribute Filter will have the Cisco ISE profiler only to keep significant attributes and discard all other attributes. Significant attributes are those used by the Cisco ISE system or those used specifically in an endpoint profiling policy or rule.

A whitelist is a set of attributes that are used in custom endpoint profiling policies for profiling endpoints, and that are essential for Change of Authorization (CoA), Bring Your Own Device (BYOD), Device Registration WebAuth (DRW), and so on to function in Cisco ISE as expected. The whitelist is always used as a criteria when ownership changes for the endpoint (when attributes are collected by multiple Policy Service nodes) even when disabled.

By default, the whitelist is disabled and the attributes are dropped only when the attribute filter is enabled. The whitelist is dynamically updated when endpoint profiling policies change including from the feed to include new attributes in the profiling policies. Any attribute that is not present in the whitelist is dropped immediately at the time of collection, and the attribute cannot participate in profiling endpoints. When combined with the buffering, the number of persistence events can be reduced.

You must ensure that the whitelist contains a set of attributes determined from the following two sources:

- A set of attributes that are used in the default profiles so that you can match endpoints to the profiles.
- A set of attributes that are essential for Change of Authorization (CoA), Bring Your Own Device (BYOD), Device Registration WebAuth (DRW), and so on to function as expected.

Table 46: Whitelist Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA-Server</td>
<td>BYODRegistration</td>
</tr>
<tr>
<td>Calling-Station-ID</td>
<td>Certificate Expiration Date</td>
</tr>
<tr>
<td>Certificate Issue Date</td>
<td>Certificate Issuer Name</td>
</tr>
<tr>
<td>Certificate Serial Number</td>
<td>Description</td>
</tr>
<tr>
<td>DestinationIP-Address</td>
<td>Device Identifier</td>
</tr>
<tr>
<td>Device Name</td>
<td>DeviceRegistrationStatus</td>
</tr>
<tr>
<td>EndPointPolicy</td>
<td>EndPointPolicyID</td>
</tr>
<tr>
<td>EndPointProfilerServer</td>
<td>EndPointSource</td>
</tr>
<tr>
<td>FQDN</td>
<td>FirstCollection</td>
</tr>
<tr>
<td>Framed-IP-Address</td>
<td>IdentityGroup</td>
</tr>
<tr>
<td>IdentityGroupID</td>
<td>IdentityStoreGUID</td>
</tr>
<tr>
<td>IdentityStoreName</td>
<td>L4_DST_PORT</td>
</tr>
</tbody>
</table>

Cisco Identity Services Engine Administrator Guide, Release 2.2 659
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LastNmapScanTime</td>
<td>MACAddress</td>
</tr>
<tr>
<td>MatchedPolicy</td>
<td>MatchedPolicyID</td>
</tr>
<tr>
<td>NADAAddress</td>
<td>NAS-IP-Address</td>
</tr>
<tr>
<td>NAS-Port-Id</td>
<td>NAS-Port-Type</td>
</tr>
<tr>
<td>NmapScanCount</td>
<td>NmapSubnetScanID</td>
</tr>
<tr>
<td>OS Version</td>
<td>OUI</td>
</tr>
<tr>
<td>PolicyVersion</td>
<td>PortalUser</td>
</tr>
<tr>
<td>PostureApplicable</td>
<td>Product</td>
</tr>
<tr>
<td>RegistrationTimeStamp</td>
<td>—</td>
</tr>
<tr>
<td>StaticAssignment</td>
<td>StaticGroupAssignment</td>
</tr>
<tr>
<td>TimeToProfile</td>
<td>Total Certainty Factor</td>
</tr>
<tr>
<td>User-Agent</td>
<td>cdpCacheAddress</td>
</tr>
<tr>
<td>cdpCacheCapabilities</td>
<td>cdpCacheDeviceId</td>
</tr>
<tr>
<td>cdpCachePlatform</td>
<td>cdpCacheVersion</td>
</tr>
<tr>
<td>ciaddr</td>
<td>dhcp-class-identifier</td>
</tr>
<tr>
<td>dhcp-requested-address</td>
<td>host-name</td>
</tr>
<tr>
<td>hrDeviceDescr</td>
<td>ifIndex</td>
</tr>
<tr>
<td>ip</td>
<td>lldpCacheCapabilities</td>
</tr>
<tr>
<td>lldpCapabilitiesMapSupported</td>
<td>lldpSystemDescription</td>
</tr>
<tr>
<td>operating-system</td>
<td>sysDescr</td>
</tr>
<tr>
<td>161-udp</td>
<td>—</td>
</tr>
</tbody>
</table>

### Attributes Collection from IOS Sensor Embedded Switches

An IOS sensor integration allows Cisco ISE run time and the Cisco ISE profiler to collect any or all of the attributes that are sent from the switch. You can collect DHCP, CDP, and LLDP attributes directly from the switch by using the RADIUS protocol. The attributes that are collected for DHCP, CDP, and LLDP are then parsed and mapped to attributes in the profiler dictionaries in the following location: **Policy > Policy Elements > Dictionaries**.

For information about the supported Catalyst platforms for Device sensors, see [https://communities.cisco.com/docs/DOC-72932](https://communities.cisco.com/docs/DOC-72932).
**IOS Sensor Embedded Network Access Devices**

Integrating IOS sensor embedded network access devices with Cisco ISE involves the following components:

- An IOS sensor
- Data collector that is embedded in the network access device (switch) for gathering DHCP, CDP, and LLDP data
- Analyzers for processing the data and determining the device-type of endpoints

There are two ways of deploying an analyzer, but they are not expected to be used in conjunction with each other:

- An analyzer can be deployed in Cisco ISE
- Analyzers can be embedded in the switch as the sensor

**Configuration Checklist for IOS Sensor-Enabled Network Access Devices**

This section summarizes a list of tasks that you must configure in the IOS sensor-enabled switches and Cisco ISE to collect DHCP, CDP, and LLDP attributes directly from the switch:

- Ensure that the RADIUS probe is enabled in Cisco ISE.
- Ensure that network access devices support an IOS sensor for collecting DHCP, CDP, and LLDP information.
- Ensure that network access devices run the following CDP and LLDP commands to capture CDP and LLDP information from endpoints:

  ```
  cdp enable
  lldp run
  ```

- Ensure that session accounting is enabled separately by using the standard AAA and RADIUS commands. For example, use the following commands:

  ```
  aaa new-model
  aaa accounting dot1x default start-stop group radius
  radius-server host <ip> auth-port <port> acct-port <port> key <shared-secret>
  radius-server vsa send accounting
  ```

- Ensure that you run IOS sensor-specific commands.

  - **Enabling Accounting Augmentation**

    You must enable the network access devices to add IOS sensor protocol data to the RADIUS accounting messages and to generate additional accounting events when it detects new sensor protocol data. This means that any RADIUS accounting message should include all CDP, LLDP, and DHCP attributes.

    Enter the following global command:

    ```
    device-sensor accounting
    ```

  - **Disabling Accounting Augmentation**
To disable (accounting) network access devices and add IOS sensor protocol data to the RADIUS accounting messages for sessions that are hosted on a given port (if the accounting feature is globally enabled), enter the following command at the appropriate port:

no device-sensor accounting

• TLV Change Tracking

By default, for each supported peer protocol, client notifications and accounting events are generated only when an incoming packet includes a type, length, and value (TLV) that has not been received previously in the context of a given session.

You must enable client notifications and accounting events for all TLV changes where there are either new TLVs, or where previously received TLVs have different values. Enter the following command:

device-sensor notify all-changes

• Be sure that you disable the IOS Device Classifier (local analyzer) in the network access devices.

Enter the following command:

no macro auto monitor

Note
This command prevents network access devices from sending two identical RADIUS accounting messages per change.

Profiler Conditions

Profiling conditions are policy elements and are similar to other conditions. However unlike authentication, authorization, and guest conditions, the profiling conditions can be based on a limited number of attributes. The Profiler Conditions page lists the attributes that are available in Cisco ISE and their description.

Profiler conditions can be one of the following:

• Cisco Provided—Cisco ISE includes predefined profiling conditions when deployed and they are identified as Cisco Provided in the Profiler Conditions page. You cannot delete Cisco Provided profiling conditions.

You can also find Cisco Provided conditions in the System profiler dictionaries in the following location: Policy > Policy Elements > Dictionaries > System.

For example, MAC dictionary. For some products, the OUI (Organizationally Unique Identifier) is an unique attribute that you can use it first for identifying the manufacturing organization of devices. It is a component of the device MAC address. The MAC dictionary contains the MACAddress and OUI attributes.

• Administrator Created—Profiler conditions that you create as an administrator of Cisco ISE or predefined profiling conditions that are duplicated are identified as Administrator Created. You can create a profiler condition of DHCP, MAC, SNMP, IP, RADIUS, NetFlow, CDP, LLDP, and NMAP types using the profiler dictionaries in the Profiler Conditions page.
Although, the recommended upper limit for the number of profiling policies is 1000, you can stretch up to 2000 profiling policies.

**Profiling Network Scan Actions**

An endpoint scan action is a configurable action that can be referred to in an endpoint profiling policy, and that is triggered when the conditions that are associated with the network scan action are met.

An endpoint scan is used to scan endpoints in order to limit resources usage in the Cisco ISE system. A network scan action scans a single endpoint, unlike resource-intensive network scans. It improves the overall classification of endpoints, and redefines an endpoint profile for an endpoint. Endpoint scans can be processed only one at a time.

You can associate a single network scan action to an endpoint profiling policy. Cisco ISE predefines three scanning types for a network scan action, which can include one or all three scanning types: for instance, an OS-scan, an SNMPPortsAndOS-scan, and a CommonPortsAndOS-scan. You cannot edit or delete OS-scan, SNMPPortsAndOS-scan, and CommonPortsAndOS-scans, which are predefined network scan actions in Cisco ISE. You can also create a new network scan action of your own.

Once an endpoint is appropriately profiled, the configured network scan action cannot be used against that endpoint. For example, scanning an Apple-Device allows you to classify the scanned endpoint to an Apple device. Once an OS-scan determines the operating system that an endpoint is running, it is no longer matched to an Apple-Device profile, but it is matched to an appropriate profile for an Apple device.

**Create a New Network Scan Action**

A network scan action that is associated with an endpoint profiling policy scans an endpoint for an operating system, Simple Network Management Protocol (SNMP) ports, and common ports. Cisco provides network scan actions for the most common NMAP scans, but you can also create one of your own.

When you create a new network scan, you define the type of information that the NMAP probe will scan for.

**Before you begin**

The Network Scan (NMAP) probe must be enabled before you can define a rule to trigger a network scan action. The procedure for that is described in [Configure Probes per Cisco ISE Node](#).

---

**Step 1** Choose **Policy > Policy Elements > Results > Profiling > Network Scan (NMAP) Actions**. Alternatively, you can choose **Work Centers > Profiler > Policy Elements > NMAP Scan Actions**.

**Step 2** Click **Add**.

**Step 3** Enter a name and description for the network scan action that you want to create.

**Step 4** Check one or more check boxes when you want to scan an endpoint for the following:

- Scan OS—To scan for an operating system
- Scan SNMP Port—To scan SNMP ports (161, 162)
- Scan Common Port—To scan common ports.
- Scan Custom Ports—To scan custom ports.
**NMAP Operating System Scan**

The operating system scan (OS-scan) type scans for an operating system (and OS version) that an endpoint is running. This is a resource intensive scan.

The NMAP tool has limitations on OS-scan which may cause unreliable results. For example, when scanning an operating system of network devices such as switches and routers, the NMAP OS-scan may provide an incorrect operating-system attribute for those devices. Cisco ISE displays the operating-system attribute, even if the accuracy is not 100%.

You should configure endpoint profiling policies that use the NMAP operating-system attribute in their rules to have low certainty value conditions (Certainty Factor values). We recommend that whenever you create an endpoint profiling policy based on the NMAP:operating-system attribute, include an AND condition to help filter out false results from NMAP.

The following NMAP command scans the operating system when you associate Scan OS with an endpoint profiling policy:

```plaintext
nmap -sS -O -F -oN /opt/CSCOcpm/logs/nmap.log -append-output -oX - <IP-address>
```

The following NMAP command scans as a subnet and sends the output to nmapSubnet.log:

```plaintext
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
   --append-output -oX - <subnet>
```

### Table 47: NMAP Commands for a Manual Subnet Scan

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-O</td>
<td>Enables OS detection</td>
</tr>
<tr>
<td>-sU</td>
<td>UDP scan</td>
</tr>
<tr>
<td>-p &lt;port ranges&gt;</td>
<td>Scans only specified ports. For example, U:161, 162</td>
</tr>
<tr>
<td>oN</td>
<td>Normal output</td>
</tr>
<tr>
<td>oX</td>
<td>XML output</td>
</tr>
</tbody>
</table>

### Operating System Ports

The following table lists the TCP ports that NMAP uses for OS scanning. In addition, NMAP uses ICMP and UDP port 51824.

<table>
<thead>
<tr>
<th>Port</th>
<th>1</th>
<th>3</th>
<th>4</th>
<th>6</th>
<th>7</th>
<th>9</th>
<th>13</th>
<th>17</th>
<th>19</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System Ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>30</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>37</td>
<td>42</td>
<td>43</td>
<td>49</td>
<td>53</td>
<td>70</td>
<td>79</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>82</td>
<td>83</td>
<td>84</td>
<td>85</td>
<td>88</td>
<td>89</td>
<td>90</td>
<td>99</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>106</td>
<td>109</td>
<td>110</td>
<td>111</td>
<td>113</td>
<td>119</td>
<td>125</td>
<td>135</td>
<td></td>
</tr>
<tr>
<td>139</td>
<td>143</td>
<td>144</td>
<td>146</td>
<td>161</td>
<td>163</td>
<td>179</td>
<td>199</td>
<td>211</td>
<td></td>
</tr>
<tr>
<td>212</td>
<td>222</td>
<td>254</td>
<td>255</td>
<td>256</td>
<td>259</td>
<td>264</td>
<td>280</td>
<td>301</td>
<td></td>
</tr>
<tr>
<td>306</td>
<td>311</td>
<td>340</td>
<td>366</td>
<td>389</td>
<td>406</td>
<td>407</td>
<td>416</td>
<td>417</td>
<td></td>
</tr>
<tr>
<td>425</td>
<td>427</td>
<td>443</td>
<td>444</td>
<td>445</td>
<td>458</td>
<td>464</td>
<td>465</td>
<td>481</td>
<td></td>
</tr>
<tr>
<td>497</td>
<td>500</td>
<td>512</td>
<td>513</td>
<td>514</td>
<td>515</td>
<td>524</td>
<td>541</td>
<td>543</td>
<td></td>
</tr>
<tr>
<td>544</td>
<td>545</td>
<td>548</td>
<td>554</td>
<td>555</td>
<td>563</td>
<td>587</td>
<td>593</td>
<td>616</td>
<td></td>
</tr>
<tr>
<td>617</td>
<td>625</td>
<td>631</td>
<td>636</td>
<td>646</td>
<td>648</td>
<td>666</td>
<td>667</td>
<td>668</td>
<td></td>
</tr>
<tr>
<td>683</td>
<td>687</td>
<td>691</td>
<td>700</td>
<td>705</td>
<td>711</td>
<td>714</td>
<td>720</td>
<td>722</td>
<td></td>
</tr>
<tr>
<td>726</td>
<td>749</td>
<td>765</td>
<td>777</td>
<td>783</td>
<td>787</td>
<td>800</td>
<td>801</td>
<td>808</td>
<td></td>
</tr>
<tr>
<td>843</td>
<td>873</td>
<td>880</td>
<td>888</td>
<td>898</td>
<td>900</td>
<td>901</td>
<td>902</td>
<td>903</td>
<td></td>
</tr>
<tr>
<td>911</td>
<td>912</td>
<td>981</td>
<td>987</td>
<td>990</td>
<td>992</td>
<td>993</td>
<td>995</td>
<td>999</td>
<td></td>
</tr>
<tr>
<td>1000</td>
<td>1001</td>
<td>1002</td>
<td>1007</td>
<td>1009</td>
<td>1010</td>
<td>1011</td>
<td>1021</td>
<td>1022</td>
<td></td>
</tr>
<tr>
<td>1023</td>
<td>1024</td>
<td>1025</td>
<td>1026</td>
<td>1027</td>
<td>1028</td>
<td>1029</td>
<td>1030</td>
<td>1031</td>
<td></td>
</tr>
<tr>
<td>1032</td>
<td>1033</td>
<td>1034</td>
<td>1035</td>
<td>1036</td>
<td>1037</td>
<td>1038</td>
<td>1039</td>
<td>1040-1100</td>
<td></td>
</tr>
<tr>
<td>1102</td>
<td>1104</td>
<td>1105</td>
<td>1106</td>
<td>1107</td>
<td>1108</td>
<td>1110</td>
<td>1111</td>
<td>1112</td>
<td></td>
</tr>
<tr>
<td>1113</td>
<td>1114</td>
<td>1117</td>
<td>1119</td>
<td>1121</td>
<td>1122</td>
<td>1123</td>
<td>1124</td>
<td>1126</td>
<td></td>
</tr>
<tr>
<td>1130</td>
<td>1131</td>
<td>1132</td>
<td>1137</td>
<td>1138</td>
<td>1141</td>
<td>1145</td>
<td>1147</td>
<td>1148</td>
<td></td>
</tr>
<tr>
<td>1149</td>
<td>1151</td>
<td>1152</td>
<td>1154</td>
<td>1163</td>
<td>1164</td>
<td>1165</td>
<td>1166</td>
<td>1169</td>
<td></td>
</tr>
<tr>
<td>1174</td>
<td>1175</td>
<td>1183</td>
<td>1185</td>
<td>1186</td>
<td>1187</td>
<td>1192</td>
<td>1198</td>
<td>1199</td>
<td></td>
</tr>
<tr>
<td>1201</td>
<td>1213</td>
<td>1216</td>
<td>1217</td>
<td>1218</td>
<td>1233</td>
<td>1234</td>
<td>1236</td>
<td>1244</td>
<td></td>
</tr>
<tr>
<td>1247</td>
<td>1248</td>
<td>1259</td>
<td>1271</td>
<td>1272</td>
<td>1277</td>
<td>1287</td>
<td>1296</td>
<td>1300</td>
<td></td>
</tr>
<tr>
<td>1301</td>
<td>1309</td>
<td>1310</td>
<td>1311</td>
<td>1322</td>
<td>1328</td>
<td>1334</td>
<td>1352</td>
<td>1417</td>
<td></td>
</tr>
<tr>
<td>1433</td>
<td>1434</td>
<td>1443</td>
<td>1455</td>
<td>1461</td>
<td>1494</td>
<td>1500</td>
<td>1501</td>
<td>1503</td>
<td></td>
</tr>
<tr>
<td>1521</td>
<td>1524</td>
<td>1533</td>
<td>1556</td>
<td>1580</td>
<td>1583</td>
<td>1594</td>
<td>1600</td>
<td>1641</td>
<td></td>
</tr>
<tr>
<td>1658</td>
<td>1666</td>
<td>1687</td>
<td>1688</td>
<td>1700</td>
<td>1717</td>
<td>1718</td>
<td>1719</td>
<td>1720</td>
<td></td>
</tr>
</tbody>
</table>
### Operating System Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Port</th>
<th>Port</th>
<th>Port</th>
<th>Port</th>
<th>Port</th>
<th>Port</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1721</td>
<td>1723</td>
<td>1755</td>
<td>1761</td>
<td>1782</td>
<td>1783</td>
<td>1801</td>
<td>1805</td>
<td>1812</td>
</tr>
<tr>
<td>1839</td>
<td>1840</td>
<td>1862</td>
<td>1863</td>
<td>1864</td>
<td>1875</td>
<td>1900</td>
<td>1914</td>
<td>1935</td>
</tr>
<tr>
<td>2022</td>
<td>2030</td>
<td>2033</td>
<td>2034</td>
<td>2035</td>
<td>2038</td>
<td>2040-2043</td>
<td>2045-2049</td>
<td>2065</td>
</tr>
<tr>
<td>2068</td>
<td>2099</td>
<td>2100</td>
<td>2103</td>
<td>2105-2107</td>
<td>2111</td>
<td>2119</td>
<td>2121</td>
<td>2126</td>
</tr>
<tr>
<td>2135</td>
<td>2144</td>
<td>2160</td>
<td>2161</td>
<td>2170</td>
<td>2179</td>
<td>2190</td>
<td>2191</td>
<td>2196</td>
</tr>
<tr>
<td>2200</td>
<td>2222</td>
<td>2251</td>
<td>2260</td>
<td>2288</td>
<td>2301</td>
<td>2323</td>
<td>2366</td>
<td>2381-2383</td>
</tr>
<tr>
<td>2393</td>
<td>2394</td>
<td>2399</td>
<td>2401</td>
<td>2492</td>
<td>2500</td>
<td>2522</td>
<td>2525</td>
<td>2557</td>
</tr>
<tr>
<td>2601</td>
<td>2602</td>
<td>2604</td>
<td>2605</td>
<td>2607</td>
<td>2608</td>
<td>2638</td>
<td>2701</td>
<td>2702</td>
</tr>
<tr>
<td>2710</td>
<td>2717</td>
<td>2718</td>
<td>2725</td>
<td>2800</td>
<td>2809</td>
<td>2811</td>
<td>2869</td>
<td>2875</td>
</tr>
<tr>
<td>2909</td>
<td>2910</td>
<td>2920</td>
<td>2967</td>
<td>2968</td>
<td>2998</td>
<td>3000</td>
<td>3001</td>
<td>3003</td>
</tr>
<tr>
<td>3005</td>
<td>3006</td>
<td>3007</td>
<td>3011</td>
<td>3013</td>
<td>3017</td>
<td>3030</td>
<td>3031</td>
<td>3052</td>
</tr>
<tr>
<td>3071</td>
<td>3077</td>
<td>3128</td>
<td>3168</td>
<td>3211</td>
<td>3221</td>
<td>3260</td>
<td>3261</td>
<td>3268</td>
</tr>
<tr>
<td>3269</td>
<td>3283</td>
<td>3300</td>
<td>3301</td>
<td>3306</td>
<td>3322</td>
<td>3323</td>
<td>3324</td>
<td>3325</td>
</tr>
<tr>
<td>3333</td>
<td>3351</td>
<td>3367</td>
<td>3369</td>
<td>3370</td>
<td>3371</td>
<td>3372</td>
<td>3389</td>
<td>3390</td>
</tr>
<tr>
<td>3404</td>
<td>3476</td>
<td>3493</td>
<td>3517</td>
<td>3527</td>
<td>3546</td>
<td>3551</td>
<td>3580</td>
<td>3659</td>
</tr>
<tr>
<td>3689</td>
<td>3690</td>
<td>3703</td>
<td>3737</td>
<td>3766</td>
<td>3784</td>
<td>3800</td>
<td>3801</td>
<td>3809</td>
</tr>
<tr>
<td>3814</td>
<td>3826</td>
<td>3827</td>
<td>3828</td>
<td>3851</td>
<td>3869</td>
<td>3871</td>
<td>3878</td>
<td>3880</td>
</tr>
<tr>
<td>3889</td>
<td>3905</td>
<td>3914</td>
<td>3918</td>
<td>3920</td>
<td>3945</td>
<td>3971</td>
<td>3986</td>
<td>3995</td>
</tr>
<tr>
<td>3998</td>
<td>4000-4006</td>
<td>4045</td>
<td>4111</td>
<td>4125</td>
<td>4126</td>
<td>4129</td>
<td>4224</td>
<td>4242</td>
</tr>
<tr>
<td>4279</td>
<td>4321</td>
<td>4343</td>
<td>4443</td>
<td>4444</td>
<td>4445</td>
<td>4446</td>
<td>4449</td>
<td>4550</td>
</tr>
<tr>
<td>4567</td>
<td>4662</td>
<td>4848</td>
<td>4899</td>
<td>4900</td>
<td>4998</td>
<td>5000-5004</td>
<td>5009</td>
<td>5030</td>
</tr>
<tr>
<td>5033</td>
<td>5050</td>
<td>5051</td>
<td>5054</td>
<td>5060</td>
<td>5061</td>
<td>5080</td>
<td>5087</td>
<td>5100</td>
</tr>
<tr>
<td>5101</td>
<td>5102</td>
<td>5120</td>
<td>5190</td>
<td>5200</td>
<td>5214</td>
<td>5221</td>
<td>5222</td>
<td>5225</td>
</tr>
<tr>
<td>5226</td>
<td>5269</td>
<td>5280</td>
<td>5298</td>
<td>5357</td>
<td>5405</td>
<td>5414</td>
<td>5431</td>
<td>5432</td>
</tr>
<tr>
<td>5440</td>
<td>5500</td>
<td>5510</td>
<td>5544</td>
<td>5550</td>
<td>5555</td>
<td>5560</td>
<td>5566</td>
<td>5631</td>
</tr>
<tr>
<td>5633</td>
<td>5666</td>
<td>5678</td>
<td>5679</td>
<td>5718</td>
<td>5730</td>
<td>5800</td>
<td>5801</td>
<td>5802</td>
</tr>
<tr>
<td>5810</td>
<td>5811</td>
<td>5815</td>
<td>5822</td>
<td>5825</td>
<td>5850</td>
<td>5859</td>
<td>5862</td>
<td>5877</td>
</tr>
<tr>
<td>5900-5907</td>
<td>5910</td>
<td>5911</td>
<td>5915</td>
<td>5922</td>
<td>5925</td>
<td>5950</td>
<td>5952</td>
<td>5959</td>
</tr>
<tr>
<td>5960-5963</td>
<td>5987-5989</td>
<td>5998-6007</td>
<td>6009</td>
<td>6025</td>
<td>6059</td>
<td>6100</td>
<td>6101</td>
<td>6106</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>-----------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>6112</td>
<td>6123</td>
<td>6129</td>
<td>6156</td>
<td>6346</td>
<td>6389</td>
<td>6502</td>
<td>6510</td>
<td>6543</td>
</tr>
<tr>
<td>6547</td>
<td>6565-6567</td>
<td>6580</td>
<td>6646</td>
<td>6666</td>
<td>6667</td>
<td>6668</td>
<td>6669</td>
<td>6689</td>
</tr>
<tr>
<td>6692</td>
<td>6699</td>
<td>6779</td>
<td>6788</td>
<td>6789</td>
<td>6792</td>
<td>6839</td>
<td>6881</td>
<td>6901</td>
</tr>
<tr>
<td>6969</td>
<td>7000</td>
<td>7001</td>
<td>7002</td>
<td>7004</td>
<td>7007</td>
<td>7019</td>
<td>7025</td>
<td>7070</td>
</tr>
<tr>
<td>7100</td>
<td>7103</td>
<td>7106</td>
<td>7200</td>
<td>7201</td>
<td>7402</td>
<td>7435</td>
<td>7443</td>
<td>7496</td>
</tr>
<tr>
<td>7512</td>
<td>7625</td>
<td>7627</td>
<td>7676</td>
<td>7741</td>
<td>7777</td>
<td>7778</td>
<td>7800</td>
<td>7911</td>
</tr>
<tr>
<td>7920</td>
<td>7921</td>
<td>7937</td>
<td>7938</td>
<td>7999</td>
<td>8000</td>
<td>8001</td>
<td>8002</td>
<td>8007</td>
</tr>
<tr>
<td>8008</td>
<td>8009</td>
<td>8010</td>
<td>8011</td>
<td>8021</td>
<td>8022</td>
<td>8031</td>
<td>8042</td>
<td>8045</td>
</tr>
<tr>
<td>8080-8090</td>
<td>8093</td>
<td>8099</td>
<td>8100</td>
<td>8180</td>
<td>8181</td>
<td>8192</td>
<td>8193</td>
<td>8194</td>
</tr>
<tr>
<td>8200</td>
<td>8222</td>
<td>8254</td>
<td>8290</td>
<td>8291</td>
<td>8292</td>
<td>8300</td>
<td>8333</td>
<td>8383</td>
</tr>
<tr>
<td>8400</td>
<td>8402</td>
<td>8443</td>
<td>8500</td>
<td>8600</td>
<td>8649</td>
<td>8651</td>
<td>8652</td>
<td>8654</td>
</tr>
<tr>
<td>8701</td>
<td>8800</td>
<td>8873</td>
<td>8888</td>
<td>8899</td>
<td>8994</td>
<td>9000</td>
<td>9001</td>
<td>9002</td>
</tr>
<tr>
<td>9003</td>
<td>9009</td>
<td>9010</td>
<td>9011</td>
<td>9040</td>
<td>9050</td>
<td>9071</td>
<td>9080</td>
<td>9081</td>
</tr>
<tr>
<td>9090</td>
<td>9091</td>
<td>9099</td>
<td>9100</td>
<td>9101</td>
<td>9102</td>
<td>9103</td>
<td>9110</td>
<td>9111</td>
</tr>
<tr>
<td>9200</td>
<td>9207</td>
<td>9220</td>
<td>9290</td>
<td>9415</td>
<td>9418</td>
<td>9485</td>
<td>9500</td>
<td>9502</td>
</tr>
<tr>
<td>9503</td>
<td>9535</td>
<td>9575</td>
<td>9593</td>
<td>9594</td>
<td>9595</td>
<td>9618</td>
<td>9666</td>
<td>9876</td>
</tr>
<tr>
<td>9877</td>
<td>9878</td>
<td>9898</td>
<td>9900</td>
<td>9917</td>
<td>9929</td>
<td>9943</td>
<td>9944</td>
<td>9968</td>
</tr>
<tr>
<td>9998</td>
<td>9999</td>
<td>10000</td>
<td>10001</td>
<td>10002</td>
<td>10003</td>
<td>10004</td>
<td>10009</td>
<td>10010</td>
</tr>
<tr>
<td>10012</td>
<td>10024</td>
<td>10025</td>
<td>10082</td>
<td>10180</td>
<td>10215</td>
<td>10243</td>
<td>10566</td>
<td>10616</td>
</tr>
<tr>
<td>10617</td>
<td>10621</td>
<td>10626</td>
<td>10628</td>
<td>10629</td>
<td>10778</td>
<td>11110</td>
<td>11111</td>
<td>11967</td>
</tr>
<tr>
<td>12000</td>
<td>12174</td>
<td>12265</td>
<td>12345</td>
<td>13456</td>
<td>13722</td>
<td>13782</td>
<td>13783</td>
<td>14000</td>
</tr>
<tr>
<td>14238</td>
<td>14441</td>
<td>14442</td>
<td>15000</td>
<td>15002</td>
<td>15003</td>
<td>15004</td>
<td>15660</td>
<td>15742</td>
</tr>
<tr>
<td>16000</td>
<td>16001</td>
<td>16012</td>
<td>16016</td>
<td>16018</td>
<td>16080</td>
<td>16113</td>
<td>16992</td>
<td>16993</td>
</tr>
<tr>
<td>17877</td>
<td>17988</td>
<td>18040</td>
<td>18101</td>
<td>18988</td>
<td>19101</td>
<td>19283</td>
<td>19315</td>
<td>19350</td>
</tr>
<tr>
<td>19780</td>
<td>19801</td>
<td>19842</td>
<td>20000</td>
<td>20005</td>
<td>20031</td>
<td>20221</td>
<td>20222</td>
<td>20828</td>
</tr>
<tr>
<td>21571</td>
<td>22939</td>
<td>23502</td>
<td>24444</td>
<td>24800</td>
<td>25734</td>
<td>25735</td>
<td>26214</td>
<td>27000</td>
</tr>
<tr>
<td>27352</td>
<td>27353</td>
<td>27355</td>
<td>27356</td>
<td>27715</td>
<td>28201</td>
<td>30000</td>
<td>30718</td>
<td>30951</td>
</tr>
<tr>
<td>31038</td>
<td>31337</td>
<td>32768</td>
<td>32769</td>
<td>32770</td>
<td>32771</td>
<td>32772</td>
<td>32773</td>
<td>32774</td>
</tr>
</tbody>
</table>
NMAP SNMP Port Scan

The SNMPPortsAndOS-scan type scans an operating system (and OS version) that an endpoint is running and triggers an SNMP Query when SNMP ports (161 and 162) are open. It can be used for endpoints that are identified and matched initially with an Unknown profile for better classification.

The following NMAP command scans SNMP ports (UDP 161 and 162) when you associate the Scan SNMP Port with an endpoint profiling policy:

`nmap -sU -pU:161,162 -oN/opt/CSCOcpm/logs/nmap.log --append-output-oX-<IP-address>`

**Table 48: NMAP Commands for an Endpoint SNMP Port Scan**

<table>
<thead>
<tr>
<th><code>-sU</code></th>
<th>UDP scan.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-p &lt;port-ranges&gt;</code></td>
<td>Scans only specified ports. For example, scans UDP ports 161 and 16.2</td>
</tr>
<tr>
<td><code>-oN</code></td>
<td>Normal output.</td>
</tr>
<tr>
<td><code>-oX</code></td>
<td>XML output.</td>
</tr>
<tr>
<td><code>-IP-address</code></td>
<td>IP-address of an endpoint that is scanned.</td>
</tr>
</tbody>
</table>

NMAP Common Ports Scan

The CommanPortsAndOS-scan type scans an operating system (and OS version) that an endpoint is running and common ports (TCP and UDP), but not SNMP ports. The following NMAP command scans common ports when you associate Scan Common Port with an endpoint profiling policy:


**Table 49: NMAP Commands for an Endpoint Common Ports Scan**

| `-sTU`          | Both TCP connect scan and UDP scan. |
Common Ports

The following table lists the common ports that NMAP uses for scanning.

<table>
<thead>
<tr>
<th>TCP Ports</th>
<th>UDP Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Ports</strong></td>
<td><strong>Service</strong></td>
</tr>
<tr>
<td>21/tcp</td>
<td>ftp</td>
</tr>
<tr>
<td>22/tcp</td>
<td>ssh</td>
</tr>
<tr>
<td>23/tcp</td>
<td>telnet</td>
</tr>
<tr>
<td>25/tcp</td>
<td>smtp</td>
</tr>
<tr>
<td>53/tcp</td>
<td>domain</td>
</tr>
<tr>
<td>80/tcp</td>
<td>http</td>
</tr>
<tr>
<td>110/tcp</td>
<td>pop3</td>
</tr>
<tr>
<td>135/tcp</td>
<td>msrpc</td>
</tr>
<tr>
<td>139/tcp</td>
<td>netbios-ssn</td>
</tr>
<tr>
<td>143/tcp</td>
<td>imap</td>
</tr>
<tr>
<td>443/tcp</td>
<td>https</td>
</tr>
<tr>
<td>445/tcp</td>
<td>microsoft-ds</td>
</tr>
<tr>
<td>3389/tcp</td>
<td>ms-term-serv</td>
</tr>
<tr>
<td>8080/tcp</td>
<td>http-proxy</td>
</tr>
</tbody>
</table>

NMAP Custom Ports Scan

In addition to the common ports, you can use custom ports (Work Centers > Profiler > Policy Elements > NMAP Scan Actions or Policy > Policy Elements > Results > Profiling > Network Scan (NMAP) Actions) to specify automatic and manual NMAP scan actions. NMAP probes collect the attributes from endpoints via the specified custom ports that are open. These attributes are updated in the endpoint's attribute list in the ISE Identities page (Work Centers > Network Access > Identities > Endpoints). You can specify up to 10 UDP and 10 TCP ports for each scan action. You cannot use the same port numbers that you have specified as common ports. Refer to the Configure Profiler Policies Using the McAfee ePolicy Orchestrator section for more information.
**NMAP Include Service Version Information Scan**

The Include Service Version Information NMAP probe automatically scans the endpoints to better classify them, by collecting information about services running on the device. The service version option can be combined with common ports or custom ports.

Example:

CLI Command: `nmap -sV -p T:8083 172.21.75.217`

Output:

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>8083/tcp</td>
<td>open</td>
<td>http</td>
<td>McAfee ePolicy Orchestrator Agent 4.8.0.1500 (ePOServerName: WIN2008EPO, AgentGuid: 1F5ED719-0A22-4F3B-BABA-00FAE756C2FE)</td>
</tr>
</tbody>
</table>

**NMAP SMB Discovery Scan**

NMAP SMB Discovery scan helps differentiate the Windows versions, and results in a better endpoint profiling. You can configure the NMAP scan action to run the SMB discovery script that is provided by NMAP.

The NMAP scan action is incorporated within the windows default policies and when the endpoint matches the policy and the scanning rule, the endpoint is scanned and the result helps to determine the exact windows version. The policy will be then configured on the feed service and new pre-defined NMAP scan is created with the SMB discovery option.

The NMAP scan action is invoked by the Microsoft-Workstation policies and the result of the scan is saved on the endpoint under the operating system attribute and leveraged to the Windows policies. You can also find the SMB Discovery script option in the manual scan on the subnet.

**Note**

For SMB discovery, be sure to enable the Windows file sharing option in the endpoint.

**SMB Discovery Attributes**

When the SMB discovery script is executed on the endpoint, new SMB discovery attributes, such as SMB.Operating-system, are added to the endpoint. These attributes are considered for updating the Windows endpoint profiling policies on the feed service. When a SMB discovery script is run, the SMB discovery attribute is prefixed with SMB, such as SMB.operating-system, SMB.lanmanager, SMB.server, SMB.fqdn, SMB.domain, SMB.workgroup, and SMB.cpe.

**Skip NMAP Host Discovery**

Scanning every port of every single IP address is a time-consuming process. Depending on the purpose of the scan, you can skip the NMAP host discovery of active endpoints.
If a NMAP scan is triggered after the classification of an endpoint, the profiler always skips the host discovery of the endpoint. However, if a manual scan action is triggered after enabling the Skip NMAP Host Discovery Scan, then host discovery is skipped.

**NMAP Scan Workflow**

Steps to be followed to perform a NMAP scan:

**Before you begin**

In order to run NMAP SMB discovery script, you must enable the file sharing in your system. Refer to the Enable File Sharing to Run NMAP SMB Discovery Script topic for an example.

<table>
<thead>
<tr>
<th>Step</th>
<th>Create an SMB Scan Action.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Configure the Profiler Policy Using the SMB Scan Action.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Add a New Condition Using the SMB Attribute.</td>
</tr>
</tbody>
</table>

**Create an SMB Scan Action**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Policy &gt; Policy Elements &gt; Results &gt; Profiling &gt; Network Scan (NMAP) Actions page.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter the Action Name and Description.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Check the Run SMB Discovery Script checkbox.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Add to create the network access users.</td>
</tr>
</tbody>
</table>
Configure the Profiler Policy Using the SMB Scan Action

Before you begin

You must create a new profiler policy to scan an endpoint with the SMB scan action. For example, you can scan a Microsoft Workstation by specifying a rule that if the DHCP class identifier contains the MSFT attribute, then a network action should be taken.

Step 1  Choose Policy > Profiling > Add page.
Step 2  Enter the Name and Description.
Step 3  In the drop-down, select the scan action (for example, SMBScanAction) that you had created.

Network Scan (NMAP) Action

What to do next

You should configure the profiler policy using the SMB scan action.
What to do next
You should add a new condition using the SMB attribute.

Add a New Condition Using the SMB Attribute

Before you begin
You should create a new profiler policy to scan the version of an endpoint. For example, you can scan for Windows 7 under the Microsoft Workstation parent policy.

Step 1  Choose Policy > Profiling > Add page.
Step 2  Enter the Name (for example, Windows-7Workstation) and Description.
Step 3  In the Network Scan (NMAP) Action drop-down, select None.
Step 4  In the Parent Policy drop-down choose the Microsoft-Workstation policy.
Enable File Sharing to Run NMAP SMB Discovery Script

Given below is an example to enable file sharing in Windows OS version 7, to run the NMAP SMB discovery script.

Step 1  Choose Control Panel > Network and Internet.

Step 2  Choose the Network and Sharing Center.

Step 3  Select Change Advanced Sharing Settings.

Step 4  Ensure that the Turn on File and Printer Sharing radio button is selected.

Step 5  Be sure that the Enable File Sharing for Devices That Use 40- or 56-bit Encryption and Turn on Password Protected Sharing radio buttons are selected.

Step 6  (Optional) Click Save Changes.

Step 7  Configure the Firewall settings.
   a) In the Control Panel, navigate to System and Security > Windows Firewall > Allow a Program Through Windows Firewall.
   b) Be sure to check the File and Printer Sharing check box.
   c) Click OK.

Step 8  Configure the shared folder.
   a) Right-click the destination folder, and select Properties.
   b) Click the Sharing tab, and click Share.
   c) In the File Sharing dialog box, add the required names and click Share.
   d) Click Done after the selected folder is shared.
e) Click Advanced Sharing and select the Share This Folder check box.
f) Click Permissions.
g) In the Permissions for Scans dialog box, choose Everyone and check the Full Control check box.
h) Click OK.

**Exclude Subnets from NMAP Scan**

You can perform an NMAP scan to identify an endpoint's OS or SNMP port.

When performing the NMAP scan, you can exclude a whole subnet or IP range that should not be scanned by NMAP. You can configure the subnet or IP range in the NMAP Scan Subnet Exclusions page (Work Centers > Profiler > Settings > NMAP Scan Subnet Exclusions). This helps limit the load on your network and saves a considerable amount of time.

For Manual NMAP scan, you can use the Run Manual NMAP Scan page (Work Centers > Profiler > Manual Scans > Manual NMAP Scan > Configure NMAP Scan Subnet Exclusions At) to specify the subnet or IP range.

**Manual NMAP Scan Settings**

You can perform a manual NMAP scan (Work Centers > Profiler > Manual Scans > Manual NMAP Scan) using the scan options that are available for automatic NMAP scan. You can choose either the scan options or the predefined ones.

**Table 51: Manual NMAP Scan Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Choose the ISE node from which the NMAP scan is run.</td>
</tr>
<tr>
<td>Manual Scan Subnet</td>
<td>Enter the range of subnet IP addresses of endpoints for which you want to run the NMAP scan.</td>
</tr>
<tr>
<td>Configure NMAP Scan Subnet Exclusions At</td>
<td>You will be directed to the Work Centers &gt; Profiler &gt; Settings &gt; NMAP Scan Subnet Exclusions page. Specify the IP address and subnet mask that should be excluded. If there is a match, the NMAP scan is not run.</td>
</tr>
<tr>
<td>NMAP Scan Subnet</td>
<td>• Specify Scan Options</td>
</tr>
<tr>
<td></td>
<td>• Or, select an Existing NMAP Scan</td>
</tr>
<tr>
<td>Specify Scan Options</td>
<td>Select the required scan options: OS, SNMP Port, Common Ports, Custom Ports, Include Service Version Information, Run SMB Discovery Script, Skip NMAP Host Discovery. Refer to the Create a New Network Scan Action topic for more information.</td>
</tr>
<tr>
<td>Select an Existing NMAP Scan</td>
<td>Displays the Existing NMAP Scan Actions drop-down that displays the default profiler NMAP scan actions.</td>
</tr>
</tbody>
</table>
Run a Manual NMAP Scan

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset to Default Scan Options</td>
<td>Click the button to restore default settings (all scan options are checked).</td>
</tr>
<tr>
<td>Save as NMAP Scan Action</td>
<td>Enter an action name and a description.</td>
</tr>
</tbody>
</table>

**Run a Manual NMAP Scan**

**Step 1** Choose Work Centers > Profiler > Manual Scans > Manual NMAP Scan.

**Step 2** In the Node drop-down, select the ISE node from which you intend to run the NMAP scan.

**Step 3** In the Manual Scan Subnet text box, enter the subnet address whose endpoints you intend to check for open ports.

**Step 4** Select the required Scan Options.
   a) Choose Specify Scan Options, and on the right side of the page, choose the required scan options. Refer to the Create a New Network Scan Action page for more information.
   b) Or, Choose Select An Existing NMAP Scan Action to select the default NMAP scan action, such as McAfeeEPOOrchestratorClientScan.

**Step 5** Click Run Scan.

**Configure Profiler Policies Using the McAfee ePolicy Orchestrator**

Cisco ISE profiling services can detect if the McAfee ePolicy Orchestrator (McAfee ePO) client is present on the endpoint. This helps in determining if a given endpoint belongs to your organization.

The entities involved in the process are the:

- ISE Server
- McAfee ePO Server
- McAfee ePO Agent

Cisco ISE provides an in-built NMAP scan action (MCAFeeEPOOrchestratorClientscan) to check if the McAfee agent is running on an endpoint using NMAP McAfee script on the configured port. You can also create new NMAP scan actions using the custom ports (for example, 8082). You can configure a new NMAP scan action using the McAfee ePO software by following the steps below:

**Step 1** Configure the McAfee ePo NMAP Scan Action.

**Step 2** Configure the McAfee ePO Agent.

**Step 3** Configure Profiler Policies Using the McAfee ePO NMAP Scan Action.

**Configure the McAfee ePo NMAP Scan Action**

**Step 1** Choose Work Centers > Profiler > Policy Elements > Network Scan (NMAP) Actions.

**Step 2** Click Add.
Step 3 Enter the **Action Name** and **Description**.

Step 4 In the **Scan Options**, check the **Custom Ports**.

Step 5 In the **Custom Ports** dialog box, add the required TCP port. The 8080 TCP port is enabled by default for McAfee ePO.

Step 6 Check the **Include Service Version Information** checkbox.

Step 7 Click **Submit**.

**What to do next**

Configure the McAfee ePO agent.

---

**Configure the McAfee ePO Agent**

**Step 1** In your McAfee ePO server, check the recommended settings to facilitate the communication between the McAfee ePO agent and the ISE server.

*Figure 51: McAfee ePO Agent Recommended Options*

**Step 2** Verify that the **Accept Connections Only From The ePO Server** is unchecked.

**What to do next**

Configure profiler policies using the McAfee ePO NMAP scan action.

---

**Configure Profiler Policies Using the McAfee ePO NMAP Scan Action**

**Step 1** Choose **Policy > Profiling > Add**.

**Step 2** Enter the **Name** and **Description**.

**Step 3** In the **Network Scan (NMAP) Action** drop-down, select the required action (for example, MCAFeeEPOOrchestratorClientscan).
Step 4  Create the parent profiler policy (for example, Microsoft-Workstation containing a rule to check if the DHCP class identifier contains the MSFT attribute).

![Profiler Policy Example](image)

Step 5  Create a new policy (for example CorporateDevice) within the parent NMAP McAfee ePO policy (for example, Microsoft-Workstation) to check if the McAfee ePO agent is installed on the endpoint.

Endpoints that meet the condition are profiled as corporate devices. You can use the policy to move endpoints profiled with McAfee ePO agent to a new VLAN.
Profiler Endpoint Custom Attributes

You can use the Endpoint Administration > Identity Management > Settings > Endpoint Custom Attributes page to assign attributes to endpoints, besides the attributes that the endpoint gathers from the probe. The endpoint custom attributes can be used in authorization policies to profile endpoints.

You can create a maximum of 100 endpoint custom attributes. The types of endpoint custom attributes supported are: Int, String, Long, Boolean, and Float.

You can add values for the endpoint custom attributes in the Context Directory > Endpoints > Endpoint Classification page.

Use cases for endpoint custom attributes include, to white list or black list devices based on certain attributes or to assign certain privileges based on the authorization.

Using Endpoint Custom Attributes in Authorization Policy

The endpoint custom attributes section allows you to configure additional attributes. Each definition consists of the attribute and type (String, Int, Boolean, Float, Long). You can profile devices using endpoint custom attributes.

Given below are the steps for creating an authorization policy using endpoint custom attributes.

Step 1

Create the endpoint custom attributes and assign values.

a) Choose Administration > Identity Management > Settings > Endpoint Custom Attributes page.
b) In the Endpoint Custom Attributes area, enter the Attribute Name (for example, deviceType), Data Type (for example, String) and Parameters.
c) Click Save.
d) Choose Context Visibility > Endpoints > Summary.
e) Assign the custom attribute values.
   • Check the required MAC address check box, and click Edit.
• Or, click the required MAC address, and in the Endpoints page, click Edit.

f) In the Edit Endpoint dialog box, in the Custom Attribute area enter the required attribute values (for example, deviceType = Apple-iPhone).
g) Click Save.

Step 2 Create an authorization policy using the custom attributes and values.
   a) Choose Policy > Policy Sets.
   b) Create the authorization policy by selecting the custom attributes from the Endpoints dictionary (for example, Rule Name: Corporate Devices, Conditions: EndPoints: deviceType Contains Apple-iPhone, Permissions: then PermitAccess).
   c) Click Save.

Related Topics
   Profiler Endpoint Custom Attributes, on page 679

Create a Profiler Condition

Endpoint profiling policies in Cisco ISE allow you to categorize discovered endpoints on your network, and assign them to specific endpoint identity groups. These endpoint profiling policies are made up of profiling conditions that Cisco ISE evaluates to categorize and group endpoints.

Before you begin
To perform the following task, you must be a Super Admin or Policy Admin.

Step 1 Choose Policy > Policy Elements > Conditions > Profiling > Add.
Step 2 Enter values for the fields as described in the Endpoint Profiling Policies Settings, on page 1085.
Step 3 Click Submit to save the profiler condition.
Step 4 Repeat this procedure to create more conditions.

Related Topics
   Profiler Conditions, on page 560

Endpoint Profiling Policy Rules

You can define a rule that allows you to choose one or more profiling conditions from the library that are previously created and saved in the policy elements library, and to associate an integer value for the certainty factor for each condition, or associate either an exception action or a network scan action for that condition. The exception action or the network scan action is used to trigger the configurable action while Cisco ISE is evaluating the profiling policies with respect to the overall classification of endpoints.

When the rules in a given policy are evaluated separately with an OR operator, the certainty metric for each rule contributes to the overall matching of the endpoint profiles into a specific category of endpoints. If the rules of an endpoint profiling policy match, then the profiling policy and the matched policy are the same for that endpoint when they are dynamically discovered on your network.
**Logically Grouped Conditions in Rules**

An endpoint profiling policy (profile) contains a single condition or a combination of multiple single conditions that are logically combined using an AND or OR operator, against which you can check, categorize, and group endpoints for a given rule in a policy.

A condition is used to check the collected endpoint attribute value against the value specified in the condition for an endpoint. If you map more than one attribute, you can logically group the conditions, which helps you to categorize endpoints on your network. You can check endpoints against one or more such conditions with a corresponding certainty metric (an integer value that you define) associated with it in a rule or trigger an exception action that is associated to the condition or a network scan action that is associated to the condition.

**Certainty Factor**

The minimum certainty metric in the profiling policy evaluates the matching profile for an endpoint. Each rule in an endpoint profiling policy has a minimum certainty metric (an integer value) associated to the profiling conditions. The certainty metric is a measure that is added for all the valid rules in an endpoint profiling policy, which measures how each condition in an endpoint profiling policy contributes to improve the overall classification of endpoints.

The certainty metric for each rule contributes to the overall matching of the endpoint profiles into a specific category of endpoints. The certainty metric for all the valid rules are added together to form the matching certainty. It must exceed the minimum certainty factor that is defined in an endpoint profiling policy. By default, the minimum certainty factor for all new profiling policy rules and predefined profiling policies is 10.

**Create Endpoint Profiling Policies**

You can use the Profiling Policies page to manage endpoint profiling policies that you create as an administrator of Cisco ISE, and also endpoint profiling profiles that are provided by Cisco ISE when deployed.

You can create new profiling policies to profile endpoints by using the following options in the New Profiler Policy page:

- Policy Enabled
- Create an Identity Group for the policy to create a matching endpoint identity group or use the endpoint identity group hierarchy
- Parent Policy
- Associated CoA Type

**Note**

When you choose to create an endpoint policy in the Profiling Policies page, do not use the Stop button on your web browsers. This action leads to the following: stops loading the New Profiler Policy page, loads other list pages and the menus within the list pages when you access them, and prevents you from performing operations on all the menus within the list pages except the Filter menus. You might need to log out of Cisco ISE, and then log in again to perform operations on all the menus within the list pages.
You can create a similar characteristic profiling policy by duplicating an endpoint profiling policy through which you can modify an existing profiling policy instead of creating a new profiling policy by redefining all conditions.

| Step 1 | Choose Policy > Profiling > Profiling Policies. |
| Step 2 | Click Add. |
| Step 3 | Enter a name and description for the new endpoint policy that you want to create. The Policy Enabled check box is checked by default to include the endpoint profiling policy for validation when you profile an endpoint. |
| Step 4 | Enter a value for the minimum certainty factor within the valid range 1 to 65535. |
| Step 5 | Click the arrow next to the Exception Action drop-down list to associate an exception action or click the arrow next to the Network Scan (NMAP) Action drop-down list to associate a network scan action. |
| Step 6 | Choose one of the following options for Create an Identity Group for the policy:  
  • Yes, create matching Identity Group  
  • No, use existing Identity Group hierarchy |
| Step 7 | Click the arrow next to the Parent Policy drop-down list to associate a parent policy to the new endpoint policy. |
| Step 8 | Choose a CoA type to be associated in the Associated CoA Type drop-down list. |
| Step 9 | Click in the rule to add conditions and associate an integer value for the certainty factor for each condition or associate either an exception action or a network scan action for that condition for the overall classification of an endpoint. |
| Step 10 | Click Submit to add an endpoint policy or click the Profiler Policy List link from the New Profiler Policy page to return to the Profiling Policies page. |

Change of Authorization Configuration per Endpoint Profiling Policy

In addition to the global configuration of change of authorization (CoA) types in Cisco ISE, you can also configure to issue a specific type of CoA associated for each endpoint profiling policy.

The global No CoA type configuration overrides each CoA type configured in an endpoint profiling policy. If the global CoA type is set other than the No CoA type, then each endpoint profiling policy is allowed to override the global CoA configuration.

When a CoA is triggered, each endpoint profiling policy can determine the actual CoA type, as follows:

• General Setting—This is the default setting for all the endpoint profiling policies that issues a CoA per global configuration.

• No CoA—This setting overrides any global configuration and disables CoA for the profile.

• Port Bounce—This setting overrides the global Port Bounce and Reauth configuration types, and issues port bounce CoA.

• Reauth—This setting overrides the global Port Bounce and Reauth configuration types, and issues reauthentication CoA.
If the profiler global CoA configuration is set to Port Bounce (or Reauth), ensure that you configure corresponding endpoint profiling policies with No CoA, the per-policy CoA option so that the BYOD flow does not break for your mobile devices.

See the summary of configuration below combined for all the CoA types and the actual CoA type issued in each case based on the global and endpoint profiling policy settings.

<table>
<thead>
<tr>
<th>Global CoA Type</th>
<th>Default CoA Type set per Policy</th>
<th>No coA Type per Policy</th>
<th>Port Bounce Type per Policy</th>
<th>Reauth Type per Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>No CoA</td>
<td>No CoA</td>
<td>No CoA</td>
<td>No CoA</td>
<td>No CoA</td>
</tr>
<tr>
<td>Port Bounce</td>
<td>Port Bounce</td>
<td>No CoA</td>
<td>Port Bounce</td>
<td>Re-Auth</td>
</tr>
<tr>
<td>Reauth</td>
<td>Reauth</td>
<td>No CoA</td>
<td>Port Bounce</td>
<td>Re-Auth</td>
</tr>
</tbody>
</table>

**Import Endpoint Profiling Policies**

You can import endpoint profiling policies from a file in XML by using the same format that you can create in the export function. If you import newly created profiling policies that have parent policies associated, then you must have defined parent policies before you define child policies.

The imported file contains the hierarchy of endpoint profiling policies that contain the parent policy first, then the profile that you imported next along with the rules and checks that are defined in the policy.

**Step 1** Choose Policy > Profiling > Profiling > Profiling Policies.
**Step 2** Click Import.
**Step 3** Click Browse to locate the file that you previously exported and want to import.
**Step 4** Click Submit.
**Step 5** Click the Profiler Policy List link to return to the Profiling Policies page.

**Export Endpoint Profiling Policies**

You can export endpoint profiling policies to other Cisco ISE deployments. Or, you can use the XML file as a template for creating your own policies to import. You can also download the file to your system in the default location, which can be used for importing later.

A dialog appears when you want to export endpoint profiling policies, which prompts you to open the profiler_policies.xml with an appropriate application or save it. This is a file in XML format that you can open in a web browser, or in other appropriate applications.
Predefined Endpoint Profiling Policies

Cisco ISE includes predefined default profiling policies when Cisco ISE is deployed, and their hierarchical construction allows you to categorize identified endpoints on your network, and assign them to a matching endpoint identity groups. Because endpoint profiling policies are hierarchical, you can find that the Profiling Policies page displays the list of generic (parent) policies for devices and child policies to which their parent policies are associated in the Profiling Policies list page.

The Profiling Policies page displays endpoint profiling policies with their names, type, description and the status, if enabled or not for validation.

The endpoint profiling policy types are classified as follows:

- Cisco Provided—Endpoint profiling policies that are predefined in Cisco ISE are identified as the Cisco Provided type.

  - Administrator Modified—Endpoint profiling policies are identified as the Administrator Modified type when you modify predefined endpoint profiling policies. Cisco ISE overwrites changes that you have made in the predefined endpoint profiling policies during upgrade.

    You can delete administrator-modified policies but Cisco ISE replaces them with up-to-date versions of Cisco-provided policies.

- Administrator Created—Endpoint profiling policies that you create or when you duplicate Cisco-provided endpoint profiling policies are identified as the Administrator Created type.

We recommend that you create a generic policy (a parent) for a set of endpoints from which its children can inherit the rules and conditions. If an endpoint has to be classified, then the endpoint profile has to first match the parent, and then its descendant (child) policies when you are profiling an endpoint.

For example, Cisco-Device is a generic endpoint profiling policy for all Cisco devices, and other policies for Cisco devices are children of Cisco-Device. If an endpoint has to be classified as a Cisco-IP-Phone 7960, then the endpoint profile for this endpoint has to first match the parent Cisco-Device policy, its child Cisco-IP-Phone policy, and then the Cisco-IP-Phone 7960 profiling policy for better classification.
Predefined Endpoint Profiling Policies Overwritten During Upgrade

You can edit existing endpoint profiling policies in the Profiling Policies page. You must also save all your configurations in a copy of the predefined endpoint profiles when you want to modify the predefined endpoint profiling policies.

During an upgrade, Cisco ISE overwrites any configuration that you have saved in the predefined endpoint profiles.

Unable to Delete Endpoint Profiling Policies

You can delete selected or all the endpoint profiling policies in the Profiling Policies page. By default, you can delete all the endpoint profiling policies from the Profiling Policies page. When you select all the endpoint profiling policies and try to delete them in the Profiling Policies page, some of them may not be deleted when the endpoint profiling policies are a parent policy mapped to other endpoint profiling policies or mapped to an authorization policy and a parent policy to other endpoint profiling policies.

For example,

- You cannot delete Cisco Provided endpoint profiling policies,
- You cannot delete a parent profile in the Profiling Policies page when an endpoint profile is defined as a parent to other endpoint profiles. For example, Cisco-Device is a parent to other endpoint profiling policies for Cisco devices.
- You cannot delete an endpoint profile when it is mapped to an authorization policy. For example, Cisco-IP-Phone is mapped to the Profiled Cisco IP Phones authorization policy, and it is a parent to other endpoint profiling policies for Cisco IP Phones.

Predefined Profiling Policies for Draeger Medical Devices

Cisco ISE contains default endpoint profiling policies that include a generic policy for Draeger medical devices, a policy for Draeger-Delta medical device, and a policy for Draeger-M300 medical device. Both the medical devices share ports 2050 and 2150, and therefore you cannot classify the Draeger-Delta and Draeger-M300 medical devices when you are using the default Draeger endpoint profiling policies.

If these Draeger devices share ports 2050 and 2150 in your environment, you must add a rule in addition to checking for the device destination IP address in the default Draeger-Delta and Draeger-M300 endpoint profiling policies so that you can distinguish these medical devices.

Cisco ISE includes the following profiling conditions that are used in the endpoint profiling policies for the Draeger medical devices:

- Draeger-Delta-PortCheck1 that contains port 2000
- Draeger-Delta-PortCheck2 that contains port 2050
- Draeger-Delta-PortCheck3 that contains port 2100
- Draeger-Delta-PortCheck4 that contains port 2150
- Draeger-M300PortCheck1 that contains port 1950
- Draeger-M300PortCheck2 that contains port 2050
Endpoint Profiling Policy for Unknown Endpoints

An endpoint that does not match existing profiles and cannot be profiled in Cisco ISE is an unknown endpoint. An unknown profile is the default system profiling policy that is assigned to an endpoint, where an attribute or a set of attributes collected for that endpoint do not match with existing profiles in Cisco ISE.

An Unknown profile is assigned in the following scenarios:

- When an endpoint is dynamically discovered in Cisco ISE, and there is no matching endpoint profiling policy for that endpoint, it is assigned to the unknown profile.
- When an endpoint is statically added in Cisco ISE, and there is no matching endpoint profiling policy for a statically added endpoint, it is assigned to the unknown profile.

If you have statically added an endpoint to your network, the statically added endpoint is not profiled by the profiling service in Cisco ISE. You can change the unknown profile later to an appropriate profile and Cisco ISE will not reassign the profiling policy that you have assigned.

Endpoint Profiling Policy for Statically Added Endpoints

For the endpoint that is statically added to be profiled, the profiling service computes a profile for the endpoint by adding a new MATCHEDPROFILE attribute to the endpoint. The computed profile is the actual profile of an endpoint if that endpoint is dynamically profiled. This allows you to find the mismatch between the computed profile for statically added endpoints and the matching profile for dynamically profiled endpoints.

Endpoint Profiling Policy for Static IP Devices

If you have an endpoint with a statically assigned IP address, you can create a profile for such static IP devices. You must enable the RADIUS probe or SNMP Query and SNMP Trap probes to profile an endpoint that has a static IP address.

Endpoint Profiling Policy Matching

Cisco ISE always considers a chosen policy for an endpoint that is the matched policy rather than an evaluated policy when the profiling conditions that are defined in one or more rules are met in a profiling policy. Here, the status of static assignment for that endpoint is set to false in the system. But, this can be set to true after it is statically reassigned to an existing profiling policy in the system, by using the static assignment feature during an endpoint editing.

The following apply to the matched policies of endpoints:

- For statically assigned endpoint, the profiling service computes the MATCHEDPROFILE.
- For dynamically assigned endpoints, the MATCHEDPROFILEs are identical to the matching endpoint profiles.

You can determine a matching profiling policy for dynamic endpoints using one or more rules that are defined in a profiling policy and assign appropriately an endpoint identity group for categorization.
When an endpoint is mapped to an existing policy, the profiling service searches the hierarchy of profiling policies for the closest parent profile that has a matching group of policies and assigns the endpoint to the appropriate endpoint policy.

**Endpoint Profiling Policies Used for Authorization**

You can use an endpoint profiling policy in authorization rules, where you can create a new condition to include a check for an endpoint profiling policy as an attribute, and the attribute value assumes the name of the endpoint profiling policy. You can select an endpoint profiling policy from the EndPoints dictionary, which includes the following attributes: PostureApplicable, EndPointPolicy, LogicalProfile, and BYODRegistration.

You can define an authorization rule that includes a combination of EndPointPolicy, BYODRegistration, and identity groups.

**Endpoint Profiling Policies Grouped into Logical Profiles**

A logical profile is a container for a category of profiles or associated profiles, irrespective of Cisco-provided or administrator-created endpoint profiling policies. An endpoint profiling policy can be associated to multiple logical profiles.

You can use the logical profile in an authorization policy condition to help create an overall network access policy for a category of profiles. You can create a simple condition for authorization, which can be included in the authorization rule. The attribute-value pair that you can use in the authorization condition is the logical profile (attribute) and the name of the logical profile (value), which can be found in the EndPoints systems dictionary.

For example, you can create a logical profile for all mobile devices like Android, Apple iPhone, or Blackberry by assigning matching endpoint profiling policies for that category to the logical profile. Cisco ISE contains IP-Phone, a default logical profile for all the IP phones, which includes IP-Phone, Cisco-IP-Phone, Nortel-IP-Phone-2000-Series, and Avaya-IP-Phone profiles.

**Create Logical Profiles**

You can create a logical profile that you can use to group a category of endpoint profiling policies, which allows you to create an overall category of profiles or associated profiles. You can also remove the endpoint profiling policies from the assigned set moving them back to the available set. For more information about Logical Profiles, see Endpoint Profiling Policies Grouped into Logical Profiles, on page 687.

---

**Step 1** Choose **Policy > Profiling > Profiling > Logical Profiles**.

**Step 2** Click **Add**.

**Step 3** Enter a name and description for the new logical profile in the text boxes for **Name** and **Description**.

**Step 4** Choose endpoint profiling policies from the **Available Policies** to assign them in a logical profile.

**Step 5** Click the right arrow to move the selected endpoint profiling policies to the **Assigned Policies**.

**Step 6** Click **Submit**.
Profiling Exception Actions

An exception action is a single configurable action that can be referred to in an endpoint profiling policy, and that is triggered when the exception conditions that are associated with the action are met.

Exception Actions can be any one of the following types:

- Cisco-provided—You cannot delete Cisco-provided exception actions. Cisco ISE triggers the following noneditable profiling exception actions from the system when you want to profile endpoints in Cisco ISE:
  - Authorization Change—The profiling service issues a change of authorization when an endpoint is added or removed from an endpoint identity group that is used by an authorization policy.
  - Endpoint Delete—An exception action is triggered in Cisco ISE and a CoA is issued when an endpoint is deleted from the system in the Endpoints page, or reassigned to the unknown profile from the edit page on a Cisco ISE network.
  - FirstTimeProfiled—An exception action is triggered in Cisco ISE and a CoA is issued when an endpoint is profiled in Cisco ISE for the first time, where the profile of that endpoint changes from an unknown profile to an existing profile but that endpoint is not successfully authenticated on a Cisco ISE network.

- Administrator-created—Cisco ISE triggers profiling exception actions that you create.

Create Exception Actions

You can define and associate one or more exception rules to a single profiling policy. This association triggers an exception action (a single configurable action) when the profiling policy matches and at least one of the exception rules matches in the profiling endpoints in Cisco ISE.

Step 1
Choose Policy > Policy Elements > Results > Profiling > Exception Actions.

Step 2
Click Add.

Step 3
Enter a name and description for the exception action in the text boxes for Name and Description.

Step 4
Check the CoA Action check box.

Step 5
Click the Policy Assignment drop-down list to choose an endpoint policy.

Step 6
Click Submit.

Cisco ISE Integration with Cisco NAC Appliance

Cisco ISE supports integration only with the Cisco Network Admission Control (NAC) Appliance Release 4.9 and is available when you have installed an Advanced or Wireless license in Cisco ISE.

The Cisco ISE profiler is similar to the Cisco Network Admission Control (NAC) Profiler that manages endpoints in a Cisco NAC deployment. This integration allows you to replace the existing Cisco NAC Profiler
that is installed in a Cisco NAC deployment. It allows you to synchronize profile names from the Cisco ISE profiler and the result of endpoint classification into the Cisco Clean Access Manager (CAM).

**Cisco Clean Access Manager Configuration in Administration Nodes**

Cisco ISE allows you to register multiple Clean Access Managers (CAMs) on the Primary PAN in a distributed deployment for REST APIs communication settings. The list of CAMs that is registered in Cisco ISE is the list to which all the profiler configuration changes are notified. The Primary PAN is responsible for all the communication between Cisco ISE and the Cisco NAC Appliance. You can configure CAMs only in the Primary PAN in Cisco ISE. The credentials that are used at the time of registering one or more CAMs in the Primary PAN are used to authenticate connectivity with CAMs.

The communication between Cisco ISE and the Cisco NAC Appliance is secure over Secure Sockets Layer (SSL). It is also bidirectional in nature, because Cisco ISE pushes the profiler configuration changes to CAMs, and CAMs periodically pull the list of MAC addresses of endpoints and their corresponding profiles and the list of all the profile names, from Cisco ISE.

You must export the contents of the X509 Certificate from the Clean Access Manager in Administration > Clean Access Manager > SSL, and import it into the Primary PAN under Administration > System > Certificates > Trusted Certificates Store in Cisco ISE for a proper secure communication between Cisco ISE and CAM.

For more information on how to set up a pair of CAMs for high availability, see the link below.

**Cisco ISE Profiler and Cisco Clean Access Manager Communication**

The Cisco ISE profiler notifies the profiler configuration changes to all the registered Clean Access Managers (CAMs) from the Primary PAN. It avoids duplicating notification in a Cisco ISE distributed deployment. It uses the REST APIs to notify the profiler configuration changes when endpoints are added or removed, and endpoint profiling policies changed, in the Cisco ISE database. During an import of endpoints, the Cisco ISE profiler notifies CAMs only after the import is complete.

The following REST API flow is implemented to push the profiler configuration changes to CAMs:

Cisco ISE profiler endpoint change push—When endpoints are profiled and there are changes in the profiles of endpoints in Cisco ISE, then the Cisco ISE profiler notifies all the registered CAMs about the changes in the endpoint profiles.

You can configure Cisco ISE in CAMs, which allows you to synchronize CAMs with Cisco ISE, depending on your Sync Settings in CAMs. You must create rules, where you can select one or more matching profiles from the list of Cisco ISE profiles and map endpoints to any one of the Access Types in CAMs. CAMs periodically retrieve endpoints and their corresponding profiles and the list of all the profile names, from the Cisco ISE profiler.

The following REST API flows are implemented to pull the profiler configuration changes from the Cisco ISE profiler:

- NAC Manager endpoint pull—Pulls the list of MAC addresses of endpoints and their corresponding profiles of known endpoints.
- NAC Manager profile pull—Pulls the profile names from the Cisco ISE profiler.

The Cisco ISE profiler notifies the Cisco ISE Monitoring persona of all the events that can be used to monitor and troubleshoot Cisco ISE and Cisco NAC Appliance Release 4.9 integration.

The Cisco ISE profiler log captures the following events for monitoring and troubleshooting integration:
**Add Cisco Clean Access Managers**

Integrating Cisco ISE with the Cisco NAC Appliance, Release 4.9 allows you to utilize the Cisco ISE profiling service in a Cisco NAC deployment to utilize the Cisco ISE profiling service in a Cisco NAC deployment.

The NAC Managers page allows you to configure multiple Cisco Access Managers (CAMs), which provides an option to filter the CAMs that you have registered. This page lists the CAMs along with their names, descriptions, IP addresses, and the status that displays whether endpoint notification is enabled or not for those CAMs.

**Step 1** Choose **Administration > Network Resources > NAC Managers**.

**Step 2** Click **Add**.

**Step 3** Enter the name for the Cisco Access Manager.

**Step 4** Click the **Status** check box to enable REST API communication from the Cisco ISE profiler that authenticates connectivity to the CAM.

**Step 5** Enter the IP address for the CAM except the following IP addresses: 0.0.0.0 and 255.255.255.255.

**Step 6** Enter the username and password of the CAM administrator that you use to log in to the user interface of the CAM.

**Step 7** Click **Submit**.

---

**Profiling Network Scan Actions**

An endpoint scan action is a configurable action that can be referred to in an endpoint profiling policy, and that is triggered when the conditions that are associated with the network scan action are met.

An endpoint scan is used to scan endpoints in order to limit resources usage in the Cisco ISE system. A network scan action scans a single endpoint, unlike resource-intensive network scans. It improves the overall classification of endpoints, and redefines an endpoint profile for an endpoint. Endpoint scans can be processed only one at a time.

You can associate a single network scan action to an endpoint profiling policy. Cisco ISE predefined three scanning types for a network scan action, which can include one or all three scanning types: for instance, an OS-scan, an SNMPPortsAndOS-scan, and a CommonPortsAndOS-scan. You cannot edit or delete OS-scan, SNMPPortsAndOS-scan, and CommonPortsAndOS-scan, which are predefined network scan actions in Cisco ISE. You can also create a new network scan action of your own.

Once an endpoint is appropriately profiled, the configured network scan action cannot be used against that endpoint. For example, scanning an Apple-Device allows you to classify the scanned endpoint to an Apple device. Once an OS-scan determines the operating system that an endpoint is running, it is no longer matched to an Apple-Device profile, but it is matched to an appropriate profile for an Apple device.

**Create a New Network Scan Action**

A network scan action that is associated with an endpoint profiling policy scans an endpoint for an operating system, Simple Network Management Protocol (SNMP) ports, and common ports. Cisco provides network scan actions for the most common NMAP scans, but you can also create one of your own.
When you create a new network scan, you define the type of information that the NMAP probe will scan for.

**Before you begin**

The Network Scan (NMAP) probe must be enabled before you can define a rule to trigger a network scan action. The procedure for that is described in Configure Probes per Cisco ISE Node.

---

**Step 1**

Choose Policy > Policy Elements > Results > Profiling > Network Scan (NMAP) Actions. Alternatively, you can choose Work Centers > Profiler > Policy Elements > NMAP Scan Actions.

**Step 2**

Click Add.

**Step 3**

Enter a name and description for the network scan action that you want to create.

**Step 4**

Check one or more check boxes when you want to scan an endpoint for the following:

- Scan OS—To scan for an operating system
- Scan SNMP Port—To scan SNMP ports (161, 162)
- Scan Common Port—To scan common ports.
- Scan Custom Ports—To scan custom ports.
- Scan Include Service Version Information—To scan the version information, which may contain detailed description of the device.
- Run SMB Discovery Script—To scan SMB ports (445 and 139) to retrieve information such as the OS and computer name.
- Skip NMAP Host Discovery—To skip the initial host discovery stage of the NMAP scan.

**Note**

The Skip NMAP Host Discovery option is selected by default for automatic NMAP scan, however, you must select it to run manual NMAP scan.

**Step 5**

Click Submit.

---

**NMAP Operating System Scan**

The operating system scan (OS-scan) type scans for an operating system (and OS version) that an endpoint is running. This is a resource intensive scan.

The NMAP tool has limitations on OS-scan which may cause unreliable results. For example, when scanning an operating system of network devices such as switches and routers, the NMAP OS-scan may provide an incorrect operating-system attribute for those devices. Cisco ISE displays the operating-system attribute, even if the accuracy is not 100%.

You should configure endpoint profiling policies that use the NMAP operating-system attribute in their rules to have low certainty value conditions (Certainty Factor values). We recommend that whenever you create an endpoint profiling policy based on the NMAP operating-system attribute, include an AND condition to help filter out false results from NMAP.

The following NMAP command scans the operating system when you associate Scan OS with an endpoint profiling policy:

```
nmap -sS -O -F -oN /opt/CSCOcpm/logs/nmap.log -append-output -oX - <IP-address>
```
The following NMAP command scans a subnet and sends the output to nmapSubnet.log:

```
nmap -O -sU -p U:161,162 -oN /opt/CSCOcpm/logs/nmapSubnet.log
   --append-output -oX - <subnet>
```

### Table 53: NMAP Commands for a Manual Subnet Scan

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-O</td>
<td>Enables OS detection</td>
</tr>
<tr>
<td>-sU</td>
<td>UDP scan</td>
</tr>
<tr>
<td>-p &lt;port ranges&gt;</td>
<td>Scans only specified ports. For example, U:161, 162</td>
</tr>
<tr>
<td>-oN</td>
<td>Normal output</td>
</tr>
<tr>
<td>-oX</td>
<td>XML output</td>
</tr>
</tbody>
</table>

### Operating System Ports

The following table lists the TCP ports that NMAP uses for OS scanning. In addition, NMAP uses ICMP and UDP port 51824.

<table>
<thead>
<tr>
<th>Port 1</th>
<th>Port 2</th>
<th>Port 3</th>
<th>Port 4</th>
<th>Port 5</th>
<th>Port 6</th>
<th>Port 7</th>
<th>Port 8</th>
<th>Port 9</th>
<th>Port 10</th>
<th>Port 11</th>
<th>Port 12</th>
<th>Port 13</th>
<th>Port 14</th>
<th>Port 15</th>
<th>Port 16</th>
<th>Port 17</th>
<th>Port 18</th>
<th>Port 19</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>4</td>
<td>6</td>
<td>7</td>
<td>9</td>
<td>13</td>
<td>17</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
<td>26</td>
<td>30</td>
<td>32</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>37</td>
<td>42</td>
<td>43</td>
<td>49</td>
<td>53</td>
<td>70</td>
<td>79</td>
<td>80</td>
<td>81</td>
<td>82</td>
<td>83</td>
<td>84</td>
<td>85</td>
<td>88</td>
<td>89</td>
<td>90</td>
<td>99</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>106</td>
<td>109</td>
<td>110</td>
<td>111</td>
<td>113</td>
<td>119</td>
<td>125</td>
<td>135</td>
<td>139</td>
<td>143</td>
<td>144</td>
<td>146</td>
<td>161</td>
<td>163</td>
<td>179</td>
<td>199</td>
<td>211</td>
<td></td>
</tr>
<tr>
<td>212</td>
<td>222</td>
<td>254</td>
<td>255</td>
<td>256</td>
<td>259</td>
<td>264</td>
<td>280</td>
<td>301</td>
<td>306</td>
<td>311</td>
<td>340</td>
<td>366</td>
<td>389</td>
<td>406</td>
<td>407</td>
<td>416</td>
<td>417</td>
<td></td>
</tr>
<tr>
<td>425</td>
<td>427</td>
<td>443</td>
<td>444</td>
<td>445</td>
<td>458</td>
<td>464</td>
<td>465</td>
<td>481</td>
<td>497</td>
<td>500</td>
<td>512</td>
<td>513</td>
<td>514</td>
<td>515</td>
<td>524</td>
<td>541</td>
<td>543</td>
<td></td>
</tr>
<tr>
<td>544</td>
<td>545</td>
<td>548</td>
<td>554</td>
<td>555</td>
<td>563</td>
<td>587</td>
<td>593</td>
<td>616</td>
<td>617</td>
<td>625</td>
<td>631</td>
<td>636</td>
<td>646</td>
<td>648</td>
<td>666</td>
<td>667</td>
<td>668</td>
<td></td>
</tr>
<tr>
<td>683</td>
<td>687</td>
<td>691</td>
<td>700</td>
<td>705</td>
<td>711</td>
<td>714</td>
<td>720</td>
<td>722</td>
<td>726</td>
<td>749</td>
<td>765</td>
<td>777</td>
<td>783</td>
<td>787</td>
<td>800</td>
<td>801</td>
<td>808</td>
<td></td>
</tr>
<tr>
<td>843</td>
<td>873</td>
<td>880</td>
<td>888</td>
<td>898</td>
<td>900</td>
<td>901</td>
<td>902</td>
<td>903</td>
<td>911</td>
<td>912</td>
<td>981</td>
<td>987</td>
<td>990</td>
<td>992</td>
<td>993</td>
<td>995</td>
<td>999</td>
<td></td>
</tr>
<tr>
<td>1000</td>
<td>1001</td>
<td>1002</td>
<td>1007</td>
<td>1009</td>
<td>1010</td>
<td>1011</td>
<td>1021</td>
<td>1022</td>
<td>1023</td>
<td>1024</td>
<td>1025</td>
<td>1026</td>
<td>1027</td>
<td>1028</td>
<td>1029</td>
<td>1030</td>
<td>1031</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Port</td>
<td>Port</td>
<td>Port</td>
<td>Port</td>
<td>Port</td>
<td>Port</td>
<td>Port</td>
<td>Port</td>
<td>Port</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1032</td>
<td>1033</td>
<td>1034</td>
<td>1035</td>
<td>1036</td>
<td>1037</td>
<td>1038</td>
<td>1039</td>
<td>1040-1100</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1102</td>
<td>1104</td>
<td>1105</td>
<td>1106</td>
<td>1107</td>
<td>1108</td>
<td>1110</td>
<td>1111</td>
<td>1112</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1113</td>
<td>1114</td>
<td>1117</td>
<td>1119</td>
<td>1121</td>
<td>1122</td>
<td>1123</td>
<td>1124</td>
<td>1126</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1130</td>
<td>1131</td>
<td>1132</td>
<td>1137</td>
<td>1138</td>
<td>1141</td>
<td>1145</td>
<td>1147</td>
<td>1148</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1149</td>
<td>1151</td>
<td>1152</td>
<td>1154</td>
<td>1163</td>
<td>1164</td>
<td>1165</td>
<td>1166</td>
<td>1169</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1174</td>
<td>1175</td>
<td>1183</td>
<td>1185</td>
<td>1186</td>
<td>1187</td>
<td>1192</td>
<td>1198</td>
<td>1199</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1201</td>
<td>1213</td>
<td>1216</td>
<td>1217</td>
<td>1218</td>
<td>1233</td>
<td>1234</td>
<td>1236</td>
<td>1244</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1247</td>
<td>1248</td>
<td>1259</td>
<td>1271</td>
<td>1272</td>
<td>1277</td>
<td>1287</td>
<td>1296</td>
<td>1300</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1301</td>
<td>1309</td>
<td>1310</td>
<td>1311</td>
<td>1322</td>
<td>1328</td>
<td>1334</td>
<td>1352</td>
<td>1417</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1433</td>
<td>1434</td>
<td>1443</td>
<td>1455</td>
<td>1461</td>
<td>1494</td>
<td>1500</td>
<td>1501</td>
<td>1503</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1521</td>
<td>1524</td>
<td>1533</td>
<td>1556</td>
<td>1580</td>
<td>1583</td>
<td>1594</td>
<td>1600</td>
<td>1641</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1658</td>
<td>1666</td>
<td>1687</td>
<td>1688</td>
<td>1700</td>
<td>1717</td>
<td>1718</td>
<td>1719</td>
<td>1720</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1721</td>
<td>1723</td>
<td>1755</td>
<td>1761</td>
<td>1782</td>
<td>1783</td>
<td>1801</td>
<td>1805</td>
<td>1812</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1839</td>
<td>1840</td>
<td>1862</td>
<td>1863</td>
<td>1864</td>
<td>1875</td>
<td>1900</td>
<td>1914</td>
<td>1935</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2022</td>
<td>2030</td>
<td>2033</td>
<td>2034</td>
<td>2035</td>
<td>2038</td>
<td>2040-2043</td>
<td>2045-2049</td>
<td>2065</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2068</td>
<td>2099</td>
<td>2100</td>
<td>2103</td>
<td>2105-2107</td>
<td>2111</td>
<td>2119</td>
<td>2121</td>
<td>2126</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2135</td>
<td>2144</td>
<td>2160</td>
<td>2161</td>
<td>2170</td>
<td>2179</td>
<td>2190</td>
<td>2191</td>
<td>2196</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2200</td>
<td>2222</td>
<td>2251</td>
<td>2260</td>
<td>2288</td>
<td>2301</td>
<td>2323</td>
<td>2366</td>
<td>2381-2383</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2393</td>
<td>2394</td>
<td>2399</td>
<td>2401</td>
<td>2492</td>
<td>2500</td>
<td>2522</td>
<td>2525</td>
<td>2557</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2601</td>
<td>2602</td>
<td>2604</td>
<td>2605</td>
<td>2607</td>
<td>2608</td>
<td>2638</td>
<td>2701</td>
<td>2702</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2710</td>
<td>2717</td>
<td>2718</td>
<td>2725</td>
<td>2800</td>
<td>2809</td>
<td>2811</td>
<td>2869</td>
<td>2875</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2909</td>
<td>2910</td>
<td>2920</td>
<td>2967</td>
<td>2968</td>
<td>2998</td>
<td>3000</td>
<td>3001</td>
<td>3003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3005</td>
<td>3006</td>
<td>3007</td>
<td>3011</td>
<td>3013</td>
<td>3017</td>
<td>3030</td>
<td>3031</td>
<td>3052</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3071</td>
<td>3077</td>
<td>3128</td>
<td>3168</td>
<td>3211</td>
<td>3221</td>
<td>3260</td>
<td>3261</td>
<td>3268</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3269</td>
<td>3283</td>
<td>3300</td>
<td>3301</td>
<td>3306</td>
<td>3322</td>
<td>3323</td>
<td>3324</td>
<td>3325</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3333</td>
<td>3351</td>
<td>3367</td>
<td>3369</td>
<td>3370</td>
<td>3371</td>
<td>3372</td>
<td>3389</td>
<td>3390</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3404</td>
<td>3476</td>
<td>3493</td>
<td>3517</td>
<td>3527</td>
<td>3546</td>
<td>3551</td>
<td>3580</td>
<td>3659</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3689</td>
<td>3690</td>
<td>3703</td>
<td>3737</td>
<td>3766</td>
<td>3784</td>
<td>3800</td>
<td>3801</td>
<td>3809</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Operating System Ports

<table>
<thead>
<tr>
<th>Port</th>
<th>Port</th>
<th>Port</th>
<th>Port</th>
<th>Port</th>
<th>Port</th>
<th>Port</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>3814</td>
<td>3826</td>
<td>3827</td>
<td>3828</td>
<td>3851</td>
<td>3869</td>
<td>3871</td>
<td>3878</td>
</tr>
<tr>
<td>3889</td>
<td>3905</td>
<td>3914</td>
<td>3918</td>
<td>3920</td>
<td>3945</td>
<td>3971</td>
<td>3986</td>
</tr>
<tr>
<td>3998</td>
<td>4000-4006</td>
<td>4045</td>
<td>4111</td>
<td>4125</td>
<td>4126</td>
<td>4129</td>
<td>4224</td>
</tr>
<tr>
<td>4279</td>
<td>4321</td>
<td>4343</td>
<td>4443</td>
<td>4444</td>
<td>4445</td>
<td>4446</td>
<td>4449</td>
</tr>
<tr>
<td>4567</td>
<td>4662</td>
<td>4848</td>
<td>4899</td>
<td>4900</td>
<td>4998</td>
<td>5000-5004</td>
<td>5009</td>
</tr>
<tr>
<td>5033</td>
<td>5050</td>
<td>5051</td>
<td>5054</td>
<td>5060</td>
<td>5061</td>
<td>5080</td>
<td>5087</td>
</tr>
<tr>
<td>5101</td>
<td>5102</td>
<td>5120</td>
<td>5190</td>
<td>5200</td>
<td>5214</td>
<td>5221</td>
<td>5222</td>
</tr>
<tr>
<td>5226</td>
<td>5269</td>
<td>5280</td>
<td>5298</td>
<td>5357</td>
<td>5405</td>
<td>5414</td>
<td>5431</td>
</tr>
<tr>
<td>5440</td>
<td>5500</td>
<td>5510</td>
<td>5544</td>
<td>5550</td>
<td>5555</td>
<td>5560</td>
<td>5566</td>
</tr>
<tr>
<td>5633</td>
<td>5666</td>
<td>5678</td>
<td>5679</td>
<td>5718</td>
<td>5730</td>
<td>5800</td>
<td>5801</td>
</tr>
<tr>
<td>5810</td>
<td>5811</td>
<td>5815</td>
<td>5822</td>
<td>5825</td>
<td>5850</td>
<td>5859</td>
<td>5862</td>
</tr>
<tr>
<td>5900-5907</td>
<td>5910</td>
<td>5911</td>
<td>5915</td>
<td>5922</td>
<td>5925</td>
<td>5950</td>
<td>5952</td>
</tr>
<tr>
<td>5960-5963</td>
<td>5987-5989</td>
<td>6009</td>
<td>6025</td>
<td>6059</td>
<td>6100</td>
<td>6101</td>
<td>6106</td>
</tr>
<tr>
<td>6112</td>
<td>6123</td>
<td>6129</td>
<td>6156</td>
<td>6346</td>
<td>6389</td>
<td>6502</td>
<td>6510</td>
</tr>
<tr>
<td>6547</td>
<td>6565-6567</td>
<td>6580</td>
<td>6646</td>
<td>6666</td>
<td>6667</td>
<td>6668</td>
<td>6669</td>
</tr>
<tr>
<td>6692</td>
<td>6699</td>
<td>6779</td>
<td>6788</td>
<td>6789</td>
<td>6792</td>
<td>6839</td>
<td>6881</td>
</tr>
<tr>
<td>6969</td>
<td>7000</td>
<td>7001</td>
<td>7002</td>
<td>7004</td>
<td>7007</td>
<td>7019</td>
<td>7025</td>
</tr>
<tr>
<td>7100</td>
<td>7103</td>
<td>7106</td>
<td>7200</td>
<td>7201</td>
<td>7402</td>
<td>7435</td>
<td>7443</td>
</tr>
<tr>
<td>7512</td>
<td>7625</td>
<td>7627</td>
<td>7676</td>
<td>7741</td>
<td>7777</td>
<td>7778</td>
<td>7800</td>
</tr>
<tr>
<td>7920</td>
<td>7921</td>
<td>7937</td>
<td>7938</td>
<td>7999</td>
<td>8000</td>
<td>8001</td>
<td>8002</td>
</tr>
<tr>
<td>8008</td>
<td>8009</td>
<td>8010</td>
<td>8011</td>
<td>8021</td>
<td>8022</td>
<td>8031</td>
<td>8042</td>
</tr>
<tr>
<td>8080-8090</td>
<td>8093</td>
<td>8099</td>
<td>8100</td>
<td>8180</td>
<td>8181</td>
<td>8192</td>
<td>8193</td>
</tr>
<tr>
<td>8200</td>
<td>8222</td>
<td>8254</td>
<td>8290</td>
<td>8291</td>
<td>8292</td>
<td>8300</td>
<td>8333</td>
</tr>
<tr>
<td>8400</td>
<td>8402</td>
<td>8443</td>
<td>8500</td>
<td>8600</td>
<td>8649</td>
<td>8651</td>
<td>8652</td>
</tr>
<tr>
<td>8701</td>
<td>8800</td>
<td>8873</td>
<td>8888</td>
<td>8899</td>
<td>8994</td>
<td>9000</td>
<td>9001</td>
</tr>
<tr>
<td>9003</td>
<td>9009</td>
<td>9010</td>
<td>9011</td>
<td>9040</td>
<td>9050</td>
<td>9071</td>
<td>9080</td>
</tr>
<tr>
<td>9090</td>
<td>9091</td>
<td>9099</td>
<td>9100</td>
<td>9101</td>
<td>9102</td>
<td>9103</td>
<td>9110</td>
</tr>
<tr>
<td>9200</td>
<td>9207</td>
<td>9220</td>
<td>9290</td>
<td>9415</td>
<td>9418</td>
<td>9485</td>
<td>9500</td>
</tr>
<tr>
<td>9503</td>
<td>9535</td>
<td>9575</td>
<td>9593</td>
<td>9594</td>
<td>9595</td>
<td>9618</td>
<td>9666</td>
</tr>
</tbody>
</table>
NMAP SNMP Port Scan

The SNMP Ports and OS scan type scans an operating system (and OS version) that an endpoint is running and triggers an SNMP Query when SNMP ports (161 and 162) are open. It can be used for endpoints that are identified and matched initially with an Unknown profile for better classification.

The following NMAP command scans SNMP ports (UDP 161 and 162) when you associate the Scan SNMP Port with an endpoint profiling policy:

```
nmap -sU -p U:161,162 -oN/opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP-address>
```
### Table 54: NMAP Commands for an Endpoint SNMP Port Scan

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-sU</code></td>
<td>UDP scan.</td>
</tr>
<tr>
<td><code>-p &lt;port-ranges&gt;</code></td>
<td>Scans only specified ports. For example, scans UDP ports 161 and 16.2</td>
</tr>
<tr>
<td><code>-oN</code></td>
<td>Normal output.</td>
</tr>
<tr>
<td><code>-oX</code></td>
<td>XML output.</td>
</tr>
<tr>
<td><code>IP-address</code></td>
<td>IP-address of an endpoint that is scanned.</td>
</tr>
</tbody>
</table>

### NMAP Common Ports Scan

The CommonPortsAndOS-scan type scans an operating system (and OS version) that an endpoint is running and common ports (TCP and UDP), but not SNMP ports. The following NMAP command scans common ports when you associate Scan Common Port with an endpoint profiling policy:

```
```

### Table 55: NMAP Commands for an Endpoint Common Ports Scan

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-sTU</code></td>
<td>Both TCP connect scan and UDP scan.</td>
</tr>
<tr>
<td><code>-oN</code></td>
<td>Normal output.</td>
</tr>
<tr>
<td><code>-oX</code></td>
<td>XML output.</td>
</tr>
<tr>
<td><code>IP address</code></td>
<td>IP address of an endpoint that is scanned.</td>
</tr>
</tbody>
</table>

### Common Ports

The following table lists the common ports that NMAP uses for scanning.

### Table 56: Common Ports

<table>
<thead>
<tr>
<th>TCP Ports</th>
<th>Service</th>
<th>UDP Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ports</td>
<td>Service</td>
<td>Ports</td>
</tr>
<tr>
<td>21/tcp</td>
<td>ftp</td>
<td>53/udp</td>
</tr>
<tr>
<td>22/tcp</td>
<td>ssh</td>
<td>67/udp</td>
</tr>
<tr>
<td>23/tcp</td>
<td>telnet</td>
<td>68/udp</td>
</tr>
<tr>
<td>25/tcp</td>
<td>smtp</td>
<td>123/udp</td>
</tr>
<tr>
<td>53/tcp</td>
<td>domain</td>
<td>135/udp</td>
</tr>
<tr>
<td>80/tcp</td>
<td>http</td>
<td>137/udp</td>
</tr>
<tr>
<td>110/tcp</td>
<td>pop3</td>
<td>138/udp</td>
</tr>
</tbody>
</table>
### NMAP Custom Ports Scan

In addition to the common ports, you can use custom ports (Work Centers > Profiler > Policy Elements > NMAP Scan Actions or Policy > Policy Elements > Results > Profiling > Network Scan (NMAP) Actions) to specify automatic and manual NMAP scan actions. NMAP probes collect the attributes from endpoints via the specified custom ports that are open. These attributes are updated in the endpoint's attribute list in the ISE Identities page (Work Centers > Network Access > Identities > Endpoints). You can specify up to 10 UDP and 10 TCP ports for each scan action. You cannot use the same port numbers that you have specified as common ports. Refer to the Configure Profiler Policies Using the McAfee ePolicy Orchestrator section for more information.

### NMAP Include Service Version Information Scan

The Include Service Version Information NMAP probe automatically scans the endpoints to better classify them, by collecting information about services running on the device. The service version option can be combined with common ports or custom ports.

Example:

CLI Command: nmap -sV -pT:8083 172.21.75.217

Output:

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>8083/tcp</td>
<td>open</td>
<td>http</td>
<td>McAfee ePolicy Orchestrator Agent 4.8.0.1500</td>
</tr>
</tbody>
</table>

### NMAP SMB Discovery Scan

NMAP SMB Discovery scan helps differentiate the Windows versions, and results in a better endpoint profiling. You can configure the NMAP scan action to run the SMB discovery script that is provided by NMAP.

The NMAP scan action is incorporated within the windows default policies and when the endpoint matches the policy and the scanning rule, the endpoint is scanned and the result helps to determine the exact windows...
version. The policy will be then configured on the feed service and new pre-defined NMAP scan is created with the SMB discovery option.

The NMAP scan action is invoked by the Microsoft-Workstation policies and the result of the scan is saved on the endpoint under the operating system attribute and leveraged to the Windows policies. You can also find the SMB Discovery script option in the manual scan on the subnet.

---

**Note**

For SMB discovery, be sure to enable the Windows file sharing option in the endpoint.

---

**SMB Discovery Attributes**

When the SMB discovery script is executed on the endpoint, new SMB discovery attributes, such as SMB.Operating-system, are added to the endpoint. These attributes are considered for updating the Windows endpoint profiling policies on the feed service. When a SMB discovery script is run, the SMB discovery attribute is prefixed with SMB, such as SMB.operating-system, SMB.lanmanager, SMB.server, SMB.fqdn, SMB.domain, SMB.workgroup, and SMB.cpe.

---

**Skip NMAP Host Discovery**

Scanning every port of every single IP address is a time-consuming process. Depending on the purpose of the scan, you can skip the NMAP host discovery of active endpoints.

If a NMAP scan is triggered after the classification of an endpoint, the profiler always skips the host discovery of the endpoint. However, if a manual scan action is triggered after enabling the Skip NMAP Host Discovery Scan, then host discovery is skipped.

---

**NMAP Scan Workflow**

Steps to be followed to perform a NMAP scan:

**Before you begin**

In order to run NMAP SMB discovery script, you must enable the file sharing in your system. Refer to the Enable File Sharing to Run NMAP SMB Discovery Script topic for an example.

---

**Step 1** Create an SMB Scan Action.

**Step 2** Configure the Profiler Policy Using the SMB Scan Action.

**Step 3** Add a New Condition Using the SMB Attribute.

---

**Create an SMB Scan Action**

**Step 1** Choose Policy > Policy Elements > Results > Profiling > Network Scan (NMAP) Actions page.

**Step 2** Enter the Action Name and Description.

**Step 3** Check the Run SMB Discovery Script checkbox.

**Step 4** Click Add to create the network access users.
What to do next

You should configure the profiler policy using the SMB scan action.

Configure the Profiler Policy Using the SMB Scan Action

Before you begin

You must create a new profiler policy to scan an endpoint with the SMB scan action. For example, you can scan a Microsoft Workstation by specifying a rule that if the DHCP class identifier contains the MSFT attribute, then a network action should be taken.

Step 1  Choose Policy > Profiling > Add page.
Step 2  Enter the Name and Description.
Step 3  In the drop-down, select the scan action (for example, SMBScanAction) that you had created.

Network Scan (NMAP) Action
Add a New Condition Using the SMB Attribute

What to do next

You should add a new condition using the SMB attribute.

Add a New Condition Using the SMB Attribute

Before you begin

You should create a new profiler policy to scan the version of an endpoint. For example, you can scan for Windows 7 under the Microsoft Workstation parent policy.

**Step 1** Choose Policy > Profiling > Add page.

**Step 2** Enter the Name (for example, Windows-7Workstation) and Description.

**Step 3** In the Network Scan (NMAP) Action drop-down, select None.

**Step 4** In the Parent Policy drop-down choose the Microsoft-Workstation policy.
Enable File Sharing to Run NMAP SMB Discovery Script

Given below is an example to enable file sharing in Windows OS version 7, to run the NMAP SMB discovery script.

**Step 1** Choose **Control Panel > Network and Internet**.

**Step 2** Choose the **Network and Sharing Center**.

**Step 3** Select **Change Advanced Sharing Settings**.

**Step 4** Ensure that the **Turn on File and Printer Sharing** radio button is selected.

**Step 5** Be sure that the **Enable File Sharing for Devices That Use 40- or 56-bit Encryption** and **Turn on Password Protected Sharing** radio buttons are selected.

**Step 6** (Optional) Click **Save Changes**.

**Step 7** Configure the Firewall settings.
   a) In the Control Panel, navigate to **System and Security > Windows Firewall > Allow a Program Through Windows Firewall**.
   b) Be sure to check the **File and Printer Sharing** check box.
   c) Click **OK**.

**Step 8** Configure the shared folder.
   a) Right-click the destination folder, and select **Properties**.
   b) Click the **Sharing** tab, and click **Share**.
   c) In the **File Sharing** dialog box, add the required names and click **Share**.
   d) Click **Done** after the selected folder is shared.
e) Click **Advanced Sharing** and select the **Share This Folder** check box.
f) Click **Permissions**.
g) In the **Permissions for Scans** dialog box, choose **Everyone** and check the **Full Control** check box.
h) Click **OK**.

---

**Exclude Subnets from NMAP Scan**

You can perform an NMAP scan to identify an endpoint's OS or SNMP port.

When performing the NMAP scan, you can exclude a whole subnet or IP range that should not be scanned by NMAP. You can configure the subnet or IP range in the NMAP Scan Subnet Exclusions page (Work Centers > Profiler > Settings > NMAP Scan Subnet Exclusions). This helps limit the load on your network and saves a considerable amount of time.

For Manual NMAP scan, you can use the Run Manual NMAP Scan page (Work Centers > Profiler > Manual Scans > Manual NMAP Scan > Configure NMAP Scan Subnet Exclusions At) to specify the subnet or IP range.

**Manual NMAP Scan Settings**

You can perform a manual NMAP scan (Work Centers > Profiler > Manual Scans > Manual NMAP Scan) using the scan options that are available for automatic NMAP scan. You can choose either the scan options or the predefined ones.

**Table 57: Manual NMAP Scan Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>Choose the ISE node from which the NMAP scan is run.</td>
</tr>
<tr>
<td>Manual Scan Subnet</td>
<td>Enter the range of subnet IP addresses of endpoints for which you want to run the NMAP scan.</td>
</tr>
<tr>
<td>Configure NMAP Scan Subnet Exclusions At</td>
<td>You will be directed to the Work Centers &gt; Profiler &gt; Settings &gt; NMAP Scan Subnet Exclusions page. Specify the IP address and subnet mask that should be excluded. If there is a match, the NMAP scan is not run.</td>
</tr>
</tbody>
</table>
| NMAP Scan Subnet | • Specify Scan Options  
  • Or, select an Existing NMAP Scan |
| Specify Scan Options | Select the required scan options: OS, SNMP Port, Common Ports, Custom Ports, Include Service Version Information, Run SMB Discovery Script, Skip NMAP Host Discovery. Refer to the Create a New Network Scan Action topic for more information. |
| Select an Existing NMAP Scan | Displays the Existing NMAP Scan Actions drop-down that displays the default profiler NMAP scan actions. |
Configure Profiler Policies Using the McAfee ePolicy Orchestrator

Cisco ISE profiling services can detect if the McAfee ePolicy Orchestrator (McAfee ePO) client is present on the endpoint. This helps in determining if a given endpoint belongs to your organization.

The entities involved in the process are the:

- ISE Server
- McAfee ePO Server
- McAfee ePO Agent

Cisco ISE provides an in-built NMAP scan action (MCAFeeEPOOrchestratorClientscan) to check if the McAfee agent is running on an endpoint using NMAP McAfee script on the configured port. You can also create new NMAP scan options using the custom ports (for example, 8082). You can configure a new NMAP scan action using the McAfee ePO software by following the steps below:

Configure the McAfee ePo NMAP Scan Action

Configure the McAfee ePO Agent.

Configure Profiler Policies Using the McAfee ePO NMAP Scan Action.

---

Run a Manual NMAP Scan

**Step 1**

**Step 2**
In the Node drop-down, select the ISE node from which you intend to run the NMAP scan.

**Step 3**
In the Manual Scan Subnet text box, enter the subnet address whose endpoints you intend to check for open ports.

**Step 4**
Select the required Scan Options.
   a) Choose Specify Scan Options, and on the right side of the page, choose the required scan options. Refer to the Create a New Network Scan Action page for more information.
   b) Or, Choose Select An Existing NMAP Scan Action to select the default NMAP scan action, such as MCAFeeEPOOrchestratorClientScan.

**Step 5**
Click Run Scan.

---

### Fields and Usage Guidelines

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reset to Default Scan Options</td>
<td>Click the button to restore default settings (all scan options are checked).</td>
</tr>
<tr>
<td>Save as NMAP Scan Action</td>
<td>Enter an action name and a description.</td>
</tr>
</tbody>
</table>
Configure the McAfee ePO Agent

Step 3 Enter the Action Name and Description.

Step 4 In the Scan Options, check the Custom Ports.

Step 5 In the Custom Ports dialog box, add the required TCP port. The 8080 TCP port is enabled by default for McAfee ePO.

Step 6 Check the Include Service Version Information checkbox.

Step 7 Click Submit.

What to do next
Configure the McAfee ePO agent.

Configure the McAfee ePO Agent

Step 1 In your McAfee ePO server, check the recommended settings to facilitate the communication between the McAfee ePO agent and the ISE server.

Step 2 Verify that the Accept Connections Only From The ePO Server is unchecked.

What to do next
Configure profiler policies using the McAfee ePO NMAP scan action.

Configure Profiler Policies Using the McAfee ePO NMAP Scan Action

Step 1 Choose Policy > Profiling > Add.

Step 2 Enter the Name and Description.

Step 3 In the Network Scan (NMAP) Action drop-down, select the required action (for example, MCAFeeEPOOrchestratorClientscan).

Step 4 Create the parent profiler policy (for example, Microsoft-Workstation containing a rule to check if the DHCP class identifier contains the MSFT attribute).
Step 5

Create a new policy (for example CorporateDevice) within the parent NMAP McAfee ePO policy (for example, Microsoft-Workstation) to check if the McAfee ePO agent is installed on the endpoint.

Endpoints that meet the condition are profiled as corporate devices. You can use the policy to move endpoints profiled with McAfee ePO agent to a new VLAN.
Profiler Endpoint Custom Attributes

You can use the Endpoint Administration > Identity Management > Settings > Endpoint Custom Attributes page to assign attributes to endpoints, besides the attributes that the endpoint gathers from the probe. The endpoint custom attributes can be used in authorization policies to profile endpoints.

You can create a maximum of 100 endpoint custom attributes. The types of endpoint custom attributes supported are: Int, String, Long, Boolean, and Float.

You can add values for the endpoint custom attributes in the Context Directory > Endpoints > Endpoint Classification page.

Use cases for endpoint custom attributes include, to white list or black list devices based on certain attributes or to assign certain privileges based on the authorization.

Using Endpoint Custom Attributes in Authorization Policy

The endpoint custom attributes section allows you to configure additional attributes. Each definition consists of the attribute and type (String, Int, Boolean, Float, Long). You can profile devices using endpoint custom attributes.

Given below are the steps for creating an authorization policy using endpoint custom attributes.

**Step 1**

Create the endpoint custom attributes and assign values.

a) Choose Administration > Identity Management > Settings > Endpoint Custom Attributes page.

b) In the Endpoint Custom Attributes area, enter the Attribute Name (for example,_deviceType), Data Type (for example, String) and Parameters.

c) Click Save.

d) Choose Context Visibility > Endpoints > Summary.

e) Assign the custom attribute values.

* Check the required MAC address check box, and click Edit.
• Or, click the required MAC address, and in the Endpoints page, click Edit.

f) In the Edit Endpoint dialog box, in the Custom Attribute area enter the required attribute values (for example, deviceType = Apple-iPhone).
g) Click Save.

**Step 2**
Create an authorization policy using the custom attributes and values.

a) Choose Policy > Policy Sets.
b) Create the authorization policy by selecting the custom attributes from the Endpoints dictionary (for example, Rule Name: Corporate Devices, Conditions: EndPoints: deviceType Contains Apple-iPhone, Permissions: then PermitAccess).
c) Click Save.

---

**Related Topics**
Profiler Endpoint Custom Attributes, on page 679

---

**Create Endpoints with Static Assignments of Policies and Identity Groups**

You can create a new endpoint statically by using the MAC address of an endpoint in the Endpoints page. You can also choose an endpoint profiling policy and an identity group in the Endpoints page for static assignment.

The regular and mobile device (MDM) endpoints are displayed in the Endpoints Identities list. In the listing page, columns for attributes like Hostname, Device Type, Device Identifier for MDM endpoints are displayed. Other columns like Static Assignment and Static Group Assignment are not displayed by default.

---

**Note**
You cannot add, edit, delete, import, or export MDM Endpoints using this page.

---

**Step 1**
Choose Work Centers > Network Access > Identities > Endpoints.

**Step 2**
Click Add.

**Step 3**
Enter the MAC address of an endpoint in hexadecimal format and separated by a colon.

**Step 4**
Choose a matching endpoint policy from the Policy Assignment drop-down list to change the static assignment status from dynamic to static.

**Step 5**
Check the Static Assignment check box to change the status of static assignment that is assigned to the endpoint from dynamic to static.

**Step 6**
Choose an endpoint identity group to which you want to assign the newly created endpoint from the Identity Group Assignment drop-down list.

**Step 7**
Check the Static Group Assignment check box to change the dynamic assignment of an endpoint identity group to static.

**Step 8**
Click Submit.
Import Endpoints from CSV Files

You can import endpoints from a CSV file that you have created from a Cisco ISE template and update it with endpoint details. Endpoints exported from ISE contains around 75 attributes and therefore cannot be imported directly into another ISE deployment. If columns that are not allowed for import are present in the CSV file, a message with the list of columns are displayed. You must delete the specified columns before trying to import the file again.

To import endpoint custom attributes, you have to create the same custom attributes as in the CSV file in the Administration > Identity Management > Settings > Endpoint Custom Attributes page using the correct data types. These attributes have to be prefixed with "CUSTOM." to differentiate them from endpoint attributes.

There are about 30 attributes that can be imported. The list includes MACAddress, EndPointPolicy, and IdentityGroup. Optional attributes are:

<table>
<thead>
<tr>
<th>Description</th>
<th>PortalUser</th>
<th>LastName</th>
</tr>
</thead>
<tbody>
<tr>
<td>PortalUser.GuestType</td>
<td>PortalUser.FirstName</td>
<td>EmailAddress</td>
</tr>
<tr>
<td>PortalUser.Location</td>
<td>Device Type</td>
<td>host-name</td>
</tr>
<tr>
<td>PortalUser.GuestStatus</td>
<td>StaticAssignment</td>
<td>Location</td>
</tr>
<tr>
<td>PortalUser CreationType</td>
<td>StaticGroupAssignment</td>
<td>MDMEnrolled</td>
</tr>
<tr>
<td>PortalUser.EmailAddress</td>
<td>User-Name</td>
<td>MDMOSVersion</td>
</tr>
<tr>
<td>PortalUser.PhoneNumber</td>
<td>DeviceRegistrationStatus</td>
<td>MDMServerName</td>
</tr>
<tr>
<td>PortalUser.LastName</td>
<td>AUPAccepted</td>
<td>MDMServerID</td>
</tr>
<tr>
<td>PortalUser.GuestSponsor</td>
<td>FirstName</td>
<td>BYODRegistration</td>
</tr>
<tr>
<td>CUSTOM.&lt;custom attribute name&gt;</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

The file header has to be in the format as specified in the default import template so that the list of endpoints appear in this order: MACAddress, EndPointPolicy, IdentityGroup <List of attributes listed above as optional attributes>. You can create the following file templates:

- MACAddress
- MACAddress, EndPointPolicy
- MACAddress, EndPointPolicy, IdentityGroup
- MACAddress, EndPointPolicy, IdentityGroup, <List of attributes listed above as optional attributes>

All attribute values, except MAC address, are optional for importing endpoints from a CSV file. If you want to import endpoints without certain values, the values are still separated by the comma.

For example,

- MAC1, Endpoint Policy1, Endpoint Identity Group1
Step 1 Choose Context Visibility > Endpoints > Import.

Step 2 Click Import From File.

Step 3 Click Browse to locate the CSV file that you have already created.

Step 4 Click Submit.

Default Import Template Available for Endpoints

You can generate a template in which you can update endpoints that can be used to import endpoints. By default, you can use the Generate a Template link to create a CSV file in the Microsoft Office Excel application and save the file locally on your system. The file can be found in Context Visibility > Endpoints > Import > Import From File. You can use the Generate a Template link to create a template, and the Cisco ISE server will display the Opening template.csv dialog. This dialog allows you to open the default template.csv file, or save the template.csv file locally on your system. If you choose to open the template.csv file from the dialog, the file opens in the Microsoft Office Excel application. The default template.csv file contains a header row that displays the MAC address, Endpoint Policy, and Endpoint Identity Group, and other optional attributes.

You must update the MAC addresses of endpoints, endpoint profiling policies, endpoint identity groups along with any of the optional attribute values you wish to import, and save the file with a new file name. This file can be used to import endpoints. See the header row in the template.csv file that is created when you use the Generate a Template link.

Table 58: CSV Template File

<table>
<thead>
<tr>
<th>MAC</th>
<th>EndpointPolicy</th>
<th>IdentityGroup</th>
<th>Other Optional Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:11:11:11:11:11</td>
<td>Android</td>
<td>Profiled</td>
<td>&lt;Empty&gt;/&lt;Value&gt;</td>
</tr>
</tbody>
</table>

Unknown Endpoints Reprofiled During Import

If the file used for import contains endpoints that have their MAC addresses, and their assigned endpoint profiling policies is the Unknown profile, then those endpoints are immediately reprofiled in Cisco ISE to the matching endpoint profiling policies during import. However, they are not statically assigned to the Unknown profile. If endpoints do not have endpoint profiling policies assigned to them in the CSV file, then they are assigned to the Unknown profile, and then reprofiled to the matching endpoint profiling policies. See below how Cisco ISE reprofiles Unknown profiles that match the Xerox_Device profile during import and also how Cisco ISE reprofiles an endpoint that is unassigned.

Table 59: Unknown Profiles: Import from a File

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Endpoint Profiling Policy Assigned Before Import in Cisco ISE</th>
<th>Endpoint Profiling Policy Assigned After Import in Cisco ISE</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:00:01:02</td>
<td>Unknown.</td>
<td>Xerox-Device</td>
</tr>
</tbody>
</table>
Endpoints with Invalid Attributes Not Imported

If any of the endpoints present in the CSV file have invalid attributes, then the endpoints are not imported and an error message is displayed.

For example, if endpoints are assigned to invalid profiles in the file used for import, then they are not imported because there are no matching profiles in Cisco ISE. See below how endpoints are not imported when they are assigned to invalid profiles in the CSV file.

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Endpoint Profiling Policy Assigned Before Import in Cisco ISE</th>
<th>Endpoint Profiling Policy Assigned After Import in Cisco ISE</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:00:01:02</td>
<td>Unknown.</td>
<td>Xerox-Device</td>
</tr>
<tr>
<td>00:00:00:00:01:05</td>
<td>If an endpoint such as 00:00:00:00:01:05 is assigned to an invalid profile other than the profiles that are available in Cisco ISE, then Cisco ISE displays a warning message that the policy name is invalid and the endpoint will not be imported.</td>
<td>The endpoint is not imported because there is no matching profile in Cisco ISE.</td>
</tr>
</tbody>
</table>

Import Endpoints from LDAP Server

You can import the MAC addresses, the associated profiles, and the endpoint identity groups of endpoints securely from an LDAP server.

Before you begin

Before you begin to import endpoints, ensure that you have installed the LDAP server.

You have to configure the connection settings and query settings before you can import from an LDAP server. If the connection settings or query settings are configured incorrectly in Cisco ISE, then the “LDAP import failed:” error message appears.

Step 1 Choose Context Visibility > Endpoints > Import > Import from LDAP.
Step 2 Enter the values for the connection settings.
Step 3 Enter the values for the query settings.

Step 4 Click Submit.

Export Endpoints with Comma-Separated Values File

You can export selected or all endpoints from a Cisco ISE server into a CSV file in which endpoints are listed with around 75 attributes along with their MAC addresses, endpoint profiling policies, and endpoint identity groups. The custom attributes created in Cisco ISE will also be exported to the CSV file and is prefixed with “CUSTOM.” to differentiate them from other endpoint attributes.

To import endpoint custom attributes exported from one deployment to another, you must create the same custom attributes in the Administration > Identity Management > Settings > Endpoint Custom Attributes page and use the same data type as specified in the original deployment.

Export All exports all the endpoints in Cisco ISE, whereas Export Selected exports only the endpoints selected by the user. By default, the profiler_endpoints.csv is the CSV file and Microsoft Office Excel is the default application to open the CSV file.

Step 1 Choose Context Visibility > Endpoints.

Step 2 Click Export, and choose one of the following:

- Export Selected—You can export only the selected endpoints in the Endpoints page.
- Export All—By default, you can export all the endpoints in the Endpoints page.

Step 3 Click OK to save the profiler_endpoints.csv file.

Identified Endpoints

Cisco ISE displays identified endpoints that connect to your network and use resources on your network in the Endpoints page. An endpoint is typically a network-capable device that connect to your network through wired and wireless network access devices and VPN. Endpoints can be personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, and so on.

The MAC address of an endpoint, expressed in hexadecimal form, is always the unique representation of an endpoint, but you can also identify an endpoint with a varying set of attributes and the values associated to them, called an attribute-value pair. You can collect a varying set of attributes for endpoints based on the endpoint capability, the capability and configuration of the network access devices and the methods (probes) that you use to collect these attributes.
Dynamically Profiled Endpoints

When endpoints are discovered on your network, they can be profiled dynamically based on the configured profiling endpoint profiling policies, and assigned to the matching endpoint identity groups depending on their profiles.

Statically Profiled Endpoints

An endpoint can be profiled statically when you create an endpoint with its MAC address and associate a profile to it along with an endpoint identity group in Cisco ISE. Cisco ISE does not reassign the profiling policy and the identity group for statically assigned endpoints.

Unknown Endpoints

If you do not have a matching profiling policy for an endpoint, you can assign an unknown profiling policy (Unknown) and the endpoint therefore will be profiled as Unknown. The endpoint profiled to the Unknown endpoint policy requires that you create a profile with an attribute or a set of attributes collected for that endpoint. The endpoint that does not match any profile is grouped within the Unknown endpoint identity group.

Identified Endpoints Locally Stored in Policy Service Nodes Database

Cisco ISE writes identified endpoints locally in the Policy Service node database. After storing endpoints locally in the database, these endpoints are then made available (remote write) in the Administration node database only when significant attributes change in the endpoints, and replicated to the other Policy Service nodes database.

The following are the significant attributes:

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

When you change endpoint profile definitions in Cisco ISE, all endpoints have to be reprofiled. A Policy Service node that collects the attributes of endpoints is responsible for reprofiling of those endpoints.

When a Policy Service node starts collecting attributes about an endpoint for which attributes were initially collected by a different Policy Service node, then the endpoint ownership changes to the current Policy Service node. The new Policy Service node will retrieve the latest attributes from the previous Policy Service node and reconcile the collected attributes with those attributes that were already collected.
When a significant attribute changes in the endpoint, attributes of the endpoint are automatically saved in the Administration node database so that you have the latest significant change in the endpoint. If the Policy Service node that owns an endpoint is not available for some reasons, then the Administrator ISE node will reprofile an endpoint that lost the owner and you have to configure a new Policy Service node for such endpoints.

**Policy Service Nodes in Cluster**

Cisco ISE uses Policy Service node group as a cluster that allows to exchange endpoint attributes when two or more nodes in the cluster collect attributes for the same endpoint. We recommend to create clusters for all Policy Service nodes that reside behind a load balancer.

If a different node other than the current owner receives attributes for the same endpoint, it sends a message across the cluster requesting the latest attributes from the current owner to merge attributes and determine if a change of ownership is needed. If you have not defined a node group in Cisco ISE, it is assumed that all nodes are within one cluster.

There are no changes made to endpoint creation and replication in Cisco ISE. Only the change of ownership for endpoints is decided based on a list of attributes (white list) used for profiling that are built from static attributes and dynamic attributes.

Upon subsequent attributes collection, the endpoint is updated on the Administration node, if anyone of the following attributes changes:

- ip
- EndpointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

When an endpoint is edited and saved in the Administration node, the attributes are retrieved from the current owner of the endpoint.

**Create Endpoint Identity Groups**

Cisco ISE groups endpoints that it discovers into the corresponding endpoint identity groups. Cisco ISE comes with several system-defined endpoint identity groups. You can also create additional endpoint identity groups from the Endpoint Identity Groups page. You can edit or delete the endpoint identity groups that you have created. You can only edit the description of the system-defined endpoint identity groups; you cannot edit the name of these groups or delete them.
Step 1 Choose Administration > Identity Management > Groups > Endpoint Identity Groups.

Step 2 Click Add.

Step 3 Enter the name for the endpoint identity group that you want to create (do not include spaces in the name of the endpoint identity group).

Step 4 Enter the description for the endpoint identity group that you want to create.

Step 5 Click the Parent Group drop-down list to choose an endpoint identity group to which you want to associate the newly created endpoint identity group.

Step 6 Click Submit.

Identified Endpoints Grouped in Endpoint Identity Groups

Cisco ISE groups discovered endpoints into their corresponding endpoint identity groups based on the endpoint profiling policies. Profiling policies are hierarchical, and they are applied at the endpoint identity groups level in Cisco ISE. By grouping endpoints to endpoint identity groups, and applying profiling policies to endpoint identity groups, Cisco ISE enables you to determine the mapping of endpoints to the endpoint profiles by checking corresponding endpoint profiling policies.

Cisco ISE creates a set of endpoint identity groups by default, and allows you to create your own identity groups to which endpoints can be assigned dynamically or statically. You can create an endpoint identity group and associate the identity group to one of the system-created identity groups. You can also assign an endpoint that you create statically to any one of the identity groups that exists in the system, and the profiling service cannot reassign the identity group.

Default Endpoint Identity Groups Created for Endpoints

Cisco ISE creates the following five endpoint identity groups by default: Blacklist, GuestEndpoints, Profiled, RegisteredDevices, and Unknown. In addition, it creates two more identity groups, such as Cisco-IP-Phone and Workstation, which are associated to the Profiled (parent) identity group. A parent group is the default identity group that exists in the system.

Cisco ISE creates the following endpoint identity groups:

- **Blacklist**—This endpoint identity group includes endpoints that are statically assigned to this group in Cisco ISE and endpoints that are blacklisted in the device registration portal. An authorization profile can be defined in Cisco ISE to permit, or deny network access to endpoints in this group.
- **GuestEndpoints**—This endpoint identity group includes endpoints that are used by guest users.
- **Profiled**—This endpoint identity group includes endpoints that match endpoint profiling policies except Cisco IP phones and workstations in Cisco ISE.
- **RegisteredDevices**—This endpoint identity group includes endpoints, which are registered devices that are added by an employee through the devices registration portal. The profiling service continues to profile these devices normally when they are assigned to this group. Endpoints are statically assigned to this group in Cisco ISE, and the profiling service cannot reassign them to any other identity group. These devices will appear like any other endpoint in the endpoints list. You can edit, delete, and blacklist these devices that you added through the device registration portal from the endpoints list in the Endpoints page in Cisco ISE. Devices that you have blacklisted in the device registration portal are assigned to the
Blacklist endpoint identity group, and an authorization profile that exists in Cisco ISE redirects blacklisted devices to an URL, which displays “Unauthorised Network Access”, a default portal page to the blacklisted devices.

- Unknown—This endpoint identity group includes endpoints that do not match any profile in Cisco ISE.

In addition to the above system created endpoint identity groups, Cisco ISE creates the following endpoint identity groups, which are associated to the Profiled identity group:

- Cisco-IP-Phone—An identity group that contains all the profiled Cisco IP phones on your network.
- Workstation—An identity group that contains all the profiled workstations on your network.

**Endpoint Identity Groups Created for Matched Endpoint Profiling Policies**

If you have an endpoint policy that matches an existing policy, then the profiling service can create a matching endpoint identity group. This identity group becomes the child of the Profiled endpoint identity group. When you create an endpoint policy, you can check the Create Matching Identity Group check box in the Profiling Policies page to create a matching endpoint identity group. You cannot delete the matching identity group unless the mapping of the profile is removed.

**Add Static Endpoints in Endpoint Identity Groups**

You can add or remove statically added endpoints in any endpoint identity group.

You can add endpoints from the Endpoints widget only to a specific identity group. If you add an endpoint to the specific endpoint identity group, then the endpoint is moved from the endpoint identity group where it was dynamically grouped earlier.

Upon removal from the endpoint identity group where you recently added an endpoint, the endpoint is reprofiled back to the appropriate identity group. You do not delete endpoints from the system but only remove them from the endpoint identity group.

---

**Step 1**
Choose Administration > Identity Management > Groups > Endpoint Identity Groups.

**Step 2**
Choose an endpoint identity group, and click Edit.

**Step 3**
Click Add.

**Step 4**
Choose an endpoint in the Endpoints widget to add the selected endpoint in the endpoint identity group.

**Step 5**
Click the Endpoint Group List link to return to the Endpoint Identity Groups page.

---

**Dynamic Endpoints Reprofiled After Adding or Removing in Identity Groups**

If an endpoint identity group assignment is not static, then endpoints are reprofiled after you add or remove them from an endpoint identity group. Endpoints that are identified dynamically by the ISE profiler appear in appropriate endpoint identity groups. If you remove dynamically added endpoints from an endpoint identity group, Cisco ISE displays a message that you have successfully removed endpoints from the identity group but reprofiles them back in the endpoint identity group.
Endpoint Identity Groups Used in Authorization Rules

You can effectively use endpoint identity groups in the authorization policies to provide appropriate network access privileges to the discovered endpoints. For example, an authorization rule for all types of Cisco IP Phones is available by default in Cisco ISE in the following location: **Policy > Policy Sets > Default > Authorization Policy**.

You must ensure that the endpoint profiling policies are either standalone policies (not a parent to other endpoint profiling policies), or their parent policies of the endpoint profiling policies are not disabled.

Profiler Feed Service

Profiler conditions, exception actions, and NMAP scan actions are classified as Cisco-provided or administrator-created (see the System Type attribute). Also, the endpoint profiling policies are classified as Cisco provided, administrator created, or administrator modified (see the System Type attribute).

You can perform different operations on the profiler conditions, exception actions, NMAP scan actions, and endpoint profiling policies depending on the System Type attribute. You cannot edit or delete Cisco-provided conditions, exception actions, and nmap scan actions. Endpoint policies that are provided by Cisco cannot be deleted. When policies are edited, they are considered as administrator-modified. When administrator-modified policies are deleted, they are replaced by the up-to-date version of the Cisco-provided policy that it was based on.

You can retrieve new and updated endpoint profiling policies and the updated OUI database as a feed from a designated Cisco feed server through a subscription in to Cisco ISE. You can also receive e-mail notifications to the e-mail address as an administrator of Cisco ISE that you have configured for applied, success, and failure messages. You can also provide additional subscriber information to receive notifications. You can send the subscriber information back to Cisco for maintaining the records and they are treated as privileged and confidential.

Cisco ISE downloads the feed service policies and OUI database updates every day at 1:00 A.M of the local Cisco ISE server time zone. Cisco ISE automatically applies these downloaded feed server policies, which also stores the set of changes so that you can revert these changes back to the previous state. When you revert from the set of changes that you last applied, endpoint profiling policies that are newly added are removed and endpoint profiling policies that are updated are reverted to the previous state. In addition, the profiler feed service is automatically disabled.

You can also update the feed services manually in offline mode. You can download the updates manually by using this option if you cannot connect your ISE deployments to Cisco feed service.

When the updates occur, only the Cisco provided profiling policies and the endpoint profiling policies which were modified by the previous update, are updated. Cisco provided disabled profiling policies are also updated but they remain disabled. Administrator Created or Administrator Modified profiling policies are not overwritten. If you want to revert any Administrator Modified endpoint profiling policy to any Cisco Provided endpoint profiling policy, then you must delete or revert the Administrator Modified endpoint profiling policy to the previous Cisco Provided endpoint profiling policy.

**Note**

Updates from the Feed Service are not allowed after the license goes Out of Compliance (OOC) for 45 days within a 60-day window period. The license is out of compliance when it has expired, or when the usage exceeds the allowed number of sessions.
OUI Feed Service

The designated Cisco feed server downloads the updated OUI database from http://standards.ieee.org/develop/regauth/oui/oui.txt, which is the list of vendors associated to the MAC OUI. The updated OUI database is available for any ISE deployment as a feed that Cisco ISE downloads to its own database. Cisco ISE updates endpoints and then starts reprofiling endpoints.

The designated Cisco feed server is located at https://ise.cisco.com:8443/feedserver/. If you have any issues accessing the service, ensure that your network security components (like a firewall or proxy server, for example) allow direct access to this URL.

Configure Profiler Feed Service

The Profiler Feed Service retrieves new and updated endpoint profiling policies and MAC OUI database updates from the Cisco Feed server. If the Feed Service is unavailable or other errors have occurred, it is reported in the Operations Audit report.

You can configure Cisco ISE to send the feed service usage report back to Cisco, which sends the following information to Cisco:

- Hostname - Cisco ISE hostname
- MaxCount - Total number of endpoints
- ProfiledCount - Profiled endpoints count
- UnknownCount - Unknown endpoints count
- MatchSystemProfilesCount - Cisco Provided profiles count
- UserCreatedProfiles - User created profiles count

You can change the CoA type in a Cisco-provided profiling policy. When the feed service updates that policy, the CoA type will not be changed, but the rest of that policy's attributes will be still be updated.

Before you begin

The Profiler feed service can only be configured from the Cisco ISE Admin portal in a distributed deployment or in a standalone ISE node.

Set up a Simple Mail Transfer Protocol (SMTP) server if you plan to send e-mail notifications from the Admin portal about feed updates(Administration > System > Settings).

To update the Feed Services online:

---

Step 1  Choose Administration > Certificates > Trusted Certificates, and check if Verisign Class 3 Public Primary Certification Authority and Verisign Class 3 Server CA - G3 are enabled.

Step 2  Choose Work Centers > Profiler > Feeds.
You can also access the option in the Administration > FeedService > Profiler page.

Step 3  Click the Online Subscription Update tab.

Step 4  Click the Test Feed Service Connection button to verify that there is a connection to the Cisco Feed Service, and that the certificate is valid.

Step 5  Check the Enable Online Subscription Update check box.
Step 6 Enter time in HH:MM format (local time zone of the Cisco ISE server). By default, Cisco ISE feed service is scheduled at 1.00 AM every day.

Step 7 Check the Notify administrator when download occurs check box and enter your e-mail address in the Administrator email address text box. Check the Provide Cisco anonymous information to help improve profiling accuracy check box, if you want to allow Cisco ISE to collect non-sensitive information (that will be used to provide better services and additional features in forthcoming releases).

Step 8 Click Save.

Step 9 Click Update Now.

Instructs Cisco ISE to contact Cisco feed server for new and updated profiles created since the last feed service update. This re-profiles all endpoints in the system, which may cause an increase the load on the system. Due to updated endpoint profiling policies, there may be changes in the authorization policy for some endpoints that are currently connected to Cisco ISE.

The Update Now button is disabled when you update new and updated profiles created since the last feed service and enabled only after the download is completed. You must navigate away from the profiler feed service Configuration page and return to this page.

---

**Related Topics**

Configure Profiler Feed Services Offline, on page 718

---

**Configure Profiler Feed Services Offline**

You can update the feed services offline when Cisco ISE is not directly connected to the Cisco feed server. You can download the offline update package from the Cisco feed server and upload it to Cisco ISE using the offline feed update. You can also set email notifications about new policies that are added to the feed server.

Configuring the profiler feed services offline involves the following tasks:

1. Download Offline Update Package
2. Apply Offline Feed Updates

---

**Download Offline Update Package**

To download offline update package:

---

**Step 1** Choose Work Centers > Profiler > Feeds.
You can also access the option in the Administration > FeedService > Profiler page.

**Step 2** Click the Offline Manual Update tab.

**Step 3** Click Download Updated Profile Policies link. You will be redirected to Feed Service Partner Portal. You can also go to https://ise.cisco.com/partner/ from your browser, to go to the feed service partner portal directly.

**Step 4** If you are a first time user, accept the terms and agreements.
An email will be triggered to Feed Services administrator to approve your request. Upon approval, you will receive a confirmation email.

**Step 5** Login to the partner portal using your Cisco.com credentials.

**Step 6** Choose Offline Feed > Download Package .
Step 7  Click Generate Package.

Step 8  Click the Click to View the Offline Update Package contents link to view all the profiles and OUIs that are included in the generated package.

- The policies under Feed Profiler 1 and Feed OUI will be downloaded to all versions of Cisco ISE.
- The policies under Feed Profiler 2 will be downloaded only to Cisco ISE Release 1.3 and later.
- The policies under Feed Profiler 3 will be downloaded only to Cisco ISE Release 2.1 and later.

Step 9  Click Download Package and save the file to your local system.

You can upload the saved file to Cisco ISE server to apply the feed updates in the downloaded package.

---

Apply Offline Feed Updates

To apply the downloaded offline feed updates:

**Before you begin**

You must have downloaded the offline update package before applying the feed updates.

---

Step 1  Choose Work Centers > Profiler > Feeds.

You can also access the option in the Administration > FeedService > Profiler page.

Step 2  Click the Offline Manual Update tab.

Step 3  Click Browse and choose the downloaded profiler feed package.

Step 4  Click Apply Update.

---

Configure Email Notifications for Profile and OUI Updates

You can configure your email address to receive notifications on profile and OUI updates.

To configure email notifications:

---

Step 1  Perform Step 1 through Step 5 in the Download Offline Update Package section to go to the Feed Service Partner Portal.

Step 2  Choose Offline Feed > Email Preferences.

Step 3  Check the Enable Notifications checkbox to receive notifications.

Step 4  Choose the number of days from the days drop-down list to set the frequency in which you want to receive the notifications on new updates.

Step 5  Enter the e-mail address/addresses and click Save.

---

Undo Feed Updates

You can revert endpoint profiling policies that were updated in the previous update and remove endpoint profiling policies and OUIs that are newly added through the previous update of the profiler feed service.
An endpoint profiling policy, if modified after an update from the feed server is not changed in the system.

**Step 1** Choose Work Centers > Profiler > Feeds.

**Step 2** Click Go to Update Report Page if you want to view the configuration changes made in the Change Configuration Audit report.

**Step 3** Click Undo Latest.

---

### Profiler Reports

Cisco ISE provides you with various reports on endpoint profiling, and troubleshooting tools that you can use to manage your network. You can generate reports for historical as well as current data. You may be able to drill down on a part of the report to view more details. For large reports, you can also schedule reports and download them in various formats.

You can run the following reports for endpoints from Operations > Reports > Endpoints and Users:

- Endpoint Session History
- Profiled Endpoint Summary
- Endpoint Profile Changes
- Top Authorizations by Endpoint
- Registered Endpoints

### Detect Anomalous Behavior of Endpoints

Cisco ISE protects your network from the illegitimate use of a MAC address. ISE detects the endpoints involved in MAC address spoofing and allows you to restrict the permission of the suspicious endpoints.

The following are the two options in the profiler configuration page for Anomalous Behavior:

- Enable Anomalous Behavior Detection
- Enable Anomalous Behavior Enforcement

If you enable Anomalous Behavior detection, Cisco ISE probes for data, and checks for any contradiction to the existing data with respect to changes in attributes related to NAS-Port-Type, DHCP Class Identifier, and Endpoint Policy. If so, an attribute called AnomalousBehavior set to true is added to the endpoint which helps you to filter and view the endpoints in the Visibility Context page. Audit logs are also generated for the respective MAC address.

When anomalous behavior detection is enabled, Cisco ISE checks if the following attributes of existing endpoints have changed:

1. Port-Type—Determines if the access method of an endpoint has changed. For example, if the same MAC address that connected via Wired Dot1x has been used for Wireless Dot1x and visa-versa.
2. DHCP Class Identifier—Determines whether the type of client or vendor of an endpoint has changed. This only applies when DHCP Class identifier attribute is populated with a certain value and is then changed to another value. If an endpoint is configured with a static IP, the DHCP Class Identifier attribute is empty in Cisco ISE. Later on, if another device spoofs the MAC address of this endpoint and uses DHCP, the Class Identifier changes from an empty value to a specific string. This will not trigger anomalous behavior detection.

3. Endpoint Policy—Determines if there are significant profile changes. For example, if the profile of an endpoint changes from a “Phone” or “Printer” to a “Workstation”.

If you enable Anomalous Behavior Enforcement, a CoA is issued upon detection of the anomalous Behavior, which can be used to re-authorize the suspicious endpoints, based on the authorization rules configured in the Profiler Configuration page.

To set the authorization policy rules for endpoints with anomalous Behavior, see .

### Set Authorization Policy Rules for Endpoints with Anomalous Behavior

You can choose the action to be taken against any endpoint with anomalous Behavior by setting the corresponding rules on the Authorization Policy page.

**Step 1** Choose Policy > Policy Sets.

**Step 2** Click the arrow icon from the View column corresponding to the Default Policy to open the Set view screen and view and manage the default authorization policy.

**Step 3** From the Actions column on any row, click the cog icon and then from the drop-down list, insert a new authorization rule by selecting any of the insert or duplicate options, as necessary.

A new row appears in the Policy Sets table.

**Step 4** Enter the Rule Name.

**Step 5** From the Conditions column, click the (+) symbol.

**Step 6** Create the required conditions in the Conditions Studio Page. In the Editor section, click the Click To Add an Attribute text box, and select the required Dictionary and Attribute (for example, Endpoints.AnomalousBehaviorEqualsTrue).

You can also drag and drop a Library condition to the Click To Add An Attribute text box.

**Step 7** Click Use to set the authorization policy rules for endpoints with anomalous behavior.

**Step 8** Click Done.

### View Endpoints with Anomalous Behavior

You can view the endpoints with anomalous behavior by using any of the following options:

- Click Anomalous Behavior from Home > Summary > Metrics. This action opens a new tab with Anomalous Behaviour column in the lower pane of the page.

- Choose Context Visibility > Endpoints > Endpoint Classification. You can view the Anomalous Behaviour column in the lower pane of the page.
Create Endpoints with Static Assignments of Policies and Identity Groups

You can create a new endpoint statically by using the MAC address of an endpoint in the Endpoints page. You can also choose an endpoint profiling policy and an identity group in the Endpoints page for static assignment.

The regular and mobile device (MDM) endpoints are displayed in the Endpoints Identities list. In the listing page, columns for attributes like Hostname, Device Type, Device Identifier for MDM endpoints are displayed. Other columns like Static Assignment and Static Group Assignment are not displayed by default.

Note: You cannot add, edit, delete, import, or export MDM Endpoints using this page.

Import Endpoints from CSV Files

You can import endpoints from a CSV file that you have created from a Cisco ISE template and update it with endpoint details. Endpoints exported from ISE contains around 75 attributes and therefore cannot be imported directly into another ISE deployment. If columns that are not allowed for import are present in the
CSV file, a message with the list of columns are displayed. You must delete the specified columns before trying to import the file again.

To import endpoint custom attributes, you have to create the same custom attributes as in the CSV file in the Administration > Identity Management > Settings > Endpoint Custom Attributes page using the correct data types. These attributes have to be prefixed with "CUSTOM." to differentiate them from endpoint attributes.

There are about 30 attributes that can be imported. The list includes MACAddress, EndPointPolicy, and IdentityGroup. Optional attributes are:

<table>
<thead>
<tr>
<th>Description</th>
<th>PortalUser</th>
<th>LastName</th>
</tr>
</thead>
<tbody>
<tr>
<td>PortalUser.GuestType</td>
<td>PortalUser.FirstName</td>
<td>EmailAddress</td>
</tr>
<tr>
<td>PortalUser.Location</td>
<td>Device Type</td>
<td>host-name</td>
</tr>
<tr>
<td>PortalUser.GuestStatus</td>
<td>StaticAssignment</td>
<td>Location</td>
</tr>
<tr>
<td>PortalUser.CreationType</td>
<td>StaticGroupAssignment</td>
<td>MDMEnrolled</td>
</tr>
<tr>
<td>PortalUser.EmailAddress</td>
<td>User-Name</td>
<td>MDMOSVersion</td>
</tr>
<tr>
<td>PortalUser.PhoneNumber</td>
<td>DeviceRegistrationStatus</td>
<td>MDMServerName</td>
</tr>
<tr>
<td>PortalUser.LastName</td>
<td>AUPAccepted</td>
<td>MDMServerID</td>
</tr>
<tr>
<td>PortalUser.GuestSponsor</td>
<td>FirstName</td>
<td>BYODRegistration</td>
</tr>
<tr>
<td>CUSTOM.&lt;custom attribute name&gt;</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

The file header has to be in the format as specified in the default import template so that the list of endpoints appear in this order: MACAddress, EndPointPolicy, IdentityGroup <List of attributes listed above as optional attributes>. You can create the following file templates:

- MACAddress
- MACAddress, EndPointPolicy
- MACAddress, EndPointPolicy, IdentityGroup
- MACAddress, EndPointPolicy, IdentityGroup, <List of attributes listed above as optional attributes>

All attribute values, except MAC address, are optional for importing endpoints from a CSV file. If you want to import endpoints without certain values, the values are still separated by the comma.

For example,

- MAC1, Endpoint Policy1, Endpoint Identity Group1
- MAC2
- MAC3, Endpoint Policy3
- MAC4, Endpoint Identity Group4
- MAC5, Endpoint Identity Group5, MyDescription, MyPortalUser, and so on
Step 1  Choose Context Visibility > Endpoints > Import.

Step 2  Click Import From File.

Step 3  Click Browse to locate the CSV file that you have already created.

Step 4  Click Submit.

Default Import Template Available for Endpoints

You can generate a template in which you can update endpoints that can be used to import endpoints. By default, you can use the Generate a Template link to create a CSV file in the Microsoft Office Excel application and save the file locally on your system. The file can be found in Context Visibility > Endpoints > Import > Import From File. You can use the Generate a Template link to create a template, and the Cisco ISE server will display the Opening template.csv dialog. This dialog allows you to open the default template.csv file, or save the template.csv file locally on your system. If you choose to open the template.csv file from the dialog, the file opens in the Microsoft Office Excel application. The default template.csv file contains a header row that displays the MAC address, Endpoint Policy, and Endpoint Identity Group, and other optional attributes.

You must update the MAC addresses of endpoints, endpoint profiling policies, endpoint identity groups along with any of the optional attribute values you wish to import, and save the file with a new file name. This file can be used to import endpoints. See the header row in the template.csv file that is created when you use the Generate a Template link.

Table 61: CSV Template File

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Endpoint Policy</th>
<th>Identity Group</th>
<th>Other Optional Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>11:11:11:11:11:11</td>
<td>Android</td>
<td>Profiled</td>
<td>&lt;Empty&gt;/&lt;Value&gt;</td>
</tr>
</tbody>
</table>

Unknown Endpoints Reprofiled During Import

If the file used for import contains endpoints that have their MAC addresses, and their assigned endpoint profiling policies is the Unknown profile, then those endpoints are immediately reprofiled in Cisco ISE to the matching endpoint profiling policies during import. However, they are not statically assigned to the Unknown profile. If endpoints do not have endpoint profiling policies assigned to them in the CSV file, then they are assigned to the Unknown profile, and then reprofiled to the matching endpoint profiling policies. See below how Cisco ISE reprofiles Unknown profiles that match the Xerox_Device profile during import and also how Cisco ISE reprofiles an endpoint that is unassigned.

Table 62: Unknown Profiles: Import from a File

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Endpoint Profiling Policy Assigned Before Import in Cisco ISE</th>
<th>Endpoint Profiling Policy Assigned After Import in Cisco ISE</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:00:01:02</td>
<td>Unknown.</td>
<td>Xerox-Device</td>
</tr>
<tr>
<td>00:00:00:00:01:03</td>
<td>Unknown.</td>
<td>Xerox-Device</td>
</tr>
<tr>
<td>00:00:00:00:01:04</td>
<td>Unknown.</td>
<td>Xerox-Device</td>
</tr>
</tbody>
</table>
Endpoints with Invalid Attributes Not Imported

If any of the endpoints present in the CSV file have invalid attributes, then the endpoints are not imported and an error message is displayed.

For example, if endpoints are assigned to invalid profiles in the file used for import, then they are not imported because there are no matching profiles in Cisco ISE. See below how endpoints are not imported when they are assigned to invalid profiles in the CSV file.

Table 63: Invalid Profiles: Import from a File

<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Endpoint Profiling Policy Assigned Before Import in Cisco ISE</th>
<th>Endpoint Profiling Policy Assigned After Import in Cisco ISE</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:00:01:02</td>
<td>Unknown.</td>
<td>Xerox-Device</td>
</tr>
<tr>
<td>00:00:00:00:01:05</td>
<td>If an endpoint such as 00:00:00:00:01:05 is assigned to an invalid profile other than the profiles that are available in Cisco ISE, then Cisco ISE displays a warning message that the policy name is invalid and the endpoint will not be imported.</td>
<td>The endpoint is not imported because there is no matching profile in Cisco ISE.</td>
</tr>
</tbody>
</table>

Import Endpoints from LDAP Server

You can import the MAC addresses, the associated profiles, and the endpoint identity groups of endpoints securely from an LDAP server.

Before you begin

Before you begin to import endpoints, ensure that you have installed the LDAP server.

You have to configure the connection settings and query settings before you can import from an LDAP server. If the connection settings or query settings are configured incorrectly in Cisco ISE, then the “LDAP import failed:” error message appears.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Context Visibility &gt; Endpoints &gt; Import &gt; Import from LDAP</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Enter the values for the connection settings.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the values for the query settings.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Submit</strong>.</td>
</tr>
</tbody>
</table>
Export Endpoints with Comma-Separated Values File

You can export selected or all endpoints from a Cisco ISE server into a CSV file in which endpoints are listed with around 75 attributes along with their MAC addresses, endpoint profiling policies, and endpoint identity groups. The custom attributes created in Cisco ISE will also be exported to the CSV file and is prefixed with "CUSTOM." to differentiate them from other endpoint attributes.

Note
To import endpoint custom attributes exported from one deployment to another, you must create the same custom attributes in the Administration > Identity Management > Settings > Endpoint Custom Attributes page and use the same data type as specified in the original deployment.

Export All exports all the endpoints in Cisco ISE, whereas Export Selected exports only the endpoints selected by the user. By default, the profiler_endpoints.csv is the CSV file and Microsoft Office Excel is the default application to open the CSV file.

Step 1
Choose Context Visibility > Endpoints.

Step 2
Click Export, and choose one of the following:

- Export Selected—You can export only the selected endpoints in the Endpoints page.

- Export All—By default, you can export all the endpoints in the Endpoints page.

Step 3
Click OK to save the profiler_endpoints.csv file.

Identified Endpoints

Cisco ISE displays identified endpoints that connect to your network and use resources on your network in the Endpoints page. An endpoint is typically a network-capable device that connect to your network through wired and wireless network access devices and VPN. Endpoints can be personal computers, laptops, IP phones, smart phones, gaming consoles, printers, fax machines, and so on.

The MAC address of an endpoint, expressed in hexadecimal form, is always the unique representation of an endpoint, but you can also identify an endpoint with a varying set of attributes and the values associated to them, called an attribute-value pair. You can collect a varying set of attributes for endpoints based on the endpoint capability, the capability and configuration of the network access devices and the methods (probes) that you use to collect these attributes.

Dynamically Profiled Endpoints

When endpoints are discovered on your network, they can be profiled dynamically based on the configured profiling endpoint profiling policies, and assigned to the matching endpoint identity groups depending on their profiles.
**Statically Profiled Endpoints**

An endpoint can be profiled statically when you create an endpoint with its MAC address and associate a profile to it along with an endpoint identity group in Cisco ISE. Cisco ISE does not reassign the profiling policy and the identity group for statically assigned endpoints.

**Unknown Endpoints**

If you do not have a matching profiling policy for an endpoint, you can assign an unknown profiling policy (Unknown) and the endpoint therefore will be profiled as Unknown. The endpoint profiled to the Unknown endpoint policy requires that you create a profile with an attribute or a set of attributes collected for that endpoint. The endpoint that does not match any profile is grouped within the Unknown endpoint identity group.

**Identified Endpoints Locally Stored in Policy Service Nodes Database**

Cisco ISE writes identified endpoints locally in the Policy Service node database. After storing endpoints locally in the database, these endpoints are then made available (remote write) in the Administration node database only when significant attributes change in the endpoints, and replicated to the other Policy Service nodes database.

The following are the significant attributes:

- **ip**
- **EndPointPolicy**
- **MatchedValue**
- **StaticAssignment**
- **StaticGroupAssignment**
- **MatchedPolicyID**
- **NmapSubnetScanID**
- **PortalUser**
- **DeviceRegistrationStatus**
- **BYODRegistration**

When you change endpoint profile definitions in Cisco ISE, all endpoints have to be repроfiled. A Policy Service node that collects the attributes of endpoints is responsible for repроfileing of those endpoints.

When a Policy Service node starts collecting attributes about an endpoint for which attributes were initially collected by a different Policy Service node, then the endpoint ownership changes to the current Policy Service node. The new Policy Service node will retrieve the latest attributes from the previous Policy Service node and reconcile the collected attributes with those attributes that were already collected.

When a significant attribute changes in the endpoint, attributes of the endpoint are automatically saved in the Administration node database so that you have the latest significant change in the endpoint. If the Policy Service node that owns an endpoint is not available for some reasons, then the Administrator ISE node will repроfile an endpoint that lost the owner and you have to configure a new Policy Service node for such endpoints.
Policy Service Nodes in Cluster

Cisco ISE uses Policy Service node group as a cluster that allows to exchange endpoint attributes when two or more nodes in the cluster collect attributes for the same endpoint. We recommend to create clusters for all Policy Service nodes that reside behind a load balancer.

If a different node other than the current owner receives attributes for the same endpoint, it sends a message across the cluster requesting the latest attributes from the current owner to merge attributes and determine if a change of ownership is needed. If you have not defined a node group in Cisco ISE, it is assumed that all nodes are within one cluster.

There are no changes made to endpoint creation and replication in Cisco ISE. Only the change of ownership for endpoints is decided based on a list of attributes (white list) used for profiling that are built from static attributes and dynamic attributes.

Upon subsequent attributes collection, the endpoint is updated on the Administration node, if anyone of the following attributes changes:

- ip
- EndPointPolicy
- MatchedValue
- StaticAssignment
- StaticGroupAssignment
- MatchedPolicyID
- NmapSubnetScanID
- PortalUser
- DeviceRegistrationStatus
- BYODRegistration

When an endpoint is edited and saved in the Administration node, the attributes are retrieved from the current owner of the endpoint.

Create Endpoint Identity Groups

Cisco ISE groups endpoints that it discovers into the corresponding endpoint identity groups. Cisco ISE comes with several system-defined endpoint identity groups. You can also create additional endpoint identity groups from the Endpoint Identity Groups page. You can edit or delete the endpoint identity groups that you have created. You can only edit the description of the system-defined endpoint identity groups; you cannot edit the name of these groups or delete them.

**Step 1**  Choose Administration > Identity Management > Groups > Endpoint Identity Groups.

**Step 2**  Click Add.

**Step 3**  Enter the name for the endpoint identity group that you want to create (do not include spaces in the name of the endpoint identity group).

**Step 4**  Enter the description for the endpoint identity group that you want to create.
Step 5 Click the Parent Group drop-down list to choose an endpoint identity group to which you want to associate the newly created endpoint identity group.

Step 6 Click Submit.

Identified Endpoints Grouped in Endpoint Identity Groups

Cisco ISE groups discovered endpoints into their corresponding endpoint identity groups based on the endpoint profiling policies. Profiling policies are hierarchical, and they are applied at the endpoint identify groups level in Cisco ISE. By grouping endpoints to endpoint identity groups, and applying profiling policies to endpoint identity groups, Cisco ISE enables you to determine the mapping of endpoints to the endpoint profiles by checking corresponding endpoint profiling policies.

Cisco ISE creates a set of endpoint identity groups by default, and allows you to create your own identity groups to which endpoints can be assigned dynamically or statically. You can create an endpoint identity group and associate the identity group to one of the system-created identity groups. You can also assign an endpoint that you create statically to any one of the identity groups that exists in the system, and the profiling service cannot reassign the identity group.

Default Endpoint Identity Groups Created for Endpoints

Cisco ISE creates the following five endpoint identity groups by default: Blacklist, GuestEndpoints, Profiled, RegisteredDevices, and Unknown. In addition, it creates two more identity groups, such as Cisco-IP-Phone and Workstation, which are associated to the Profiled (parent) identity group. A parent group is the default identity group that exists in the system.

Cisco ISE creates the following endpoint identity groups:

- **Blacklist**—This endpoint identity group includes endpoints that are statically assigned to this group in Cisco ISE and endpoints that are blacklisted in the device registration portal. An authorization profile can be defined in Cisco ISE to permit, or deny network access to endpoints in this group.

- **GuestEndpoints**—This endpoint identity group includes endpoints that are used by guest users.

- **Profiled**—This endpoint identity group includes endpoints that match endpoint profiling policies except Cisco IP phones and workstations in Cisco ISE.

- **RegisteredDevices**—This endpoint identity group includes endpoints, which are registered devices that are added by an employee through the devices registration portal. The profiling service continues to profile these devices normally when they are assigned to this group. Endpoints are statically assigned to this group in Cisco ISE, and the profiling service cannot reassign them to any other identity group. These devices will appear like any other endpoint in the endpoints list. You can edit, delete, and blacklist these devices that you added through the device registration portal from the endpoints list in the Endpoints page in Cisco ISE. Devices that you have blacklisted in the device registration portal are assigned to the Blacklist endpoint identity group, and an authorization profile that exists in Cisco ISE redirects blacklisted devices to an URL, which displays “Unauthorised Network Access”, a default portal page to the blacklisted devices.

- **Unknown**—This endpoint identity group includes endpoints that do not match any profile in Cisco ISE.

In addition to the above system created endpoint identity groups, Cisco ISE creates the following endpoint identity groups, which are associated to the Profiled identity group:

- **Cisco-IP-Phone**—An identity group that contains all the profiled Cisco IP phones on your network.
• Workstation—An identity group that contains all the profiled workstations on your network.

Endpoint Identity Groups Created for Matched Endpoint Profiling Policies

If you have an endpoint policy that matches an existing policy, then the profiling service can create a matching endpoint identity group. This identity group becomes the child of the Profiled endpoint identity group. When you create an endpoint policy, you can check the Create Matching Identity Group check box in the Profiling Policies page to create a matching endpoint identity group. You cannot delete the matching identity group unless the mapping of the profile is removed.

Add Static Endpoints in Endpoint Identity Groups

You can add or remove statically added endpoints in any endpoint identity group.

You can add endpoints from the Endpoints widget only to a specific identity group. If you add an endpoint to the specific endpoint identity group, then the endpoint is moved from the endpoint identity group where it was dynamically grouped earlier.

Upon removal from the endpoint identity group where you recently added an endpoint, the endpoint is reprofiled back to the appropriate identity group. You do not delete endpoints from the system but only remove them from the endpoint identity group.

Step 1  Choose Administration > Identity Management > Groups > Endpoint Identity Groups.
Step 2  Choose an endpoint identity group, and click Edit.
Step 3  Click Add.
Step 4  Choose an endpoint in the Endpoints widget to add the selected endpoint in the endpoint identity group.
Step 5  Click the Endpoint Group List link to return to the Endpoint Identity Groups page.

Dynamic Endpoints Reprofiled After Adding or Removing in Identity Groups

If an endpoint identity group assignment is not static, then endpoints are reprofiled after you add or remove them from an endpoint identity group. Endpoints that are identified dynamically by the ISE profiler appear in appropriate endpoint identity groups. If you remove dynamically added endpoints from an endpoint identity group, Cisco ISE displays a message that you have successfully removed endpoints from the identity group but reprofiles them back in the endpoint identity group.

Endpoint Identity Groups Used in Authorization Rules

You can effectively use endpoint identity groups in the authorization policies to provide appropriate network access privileges to the discovered endpoints. For example, an authorization rule for all types of Cisco IP Phones is available by default in Cisco ISE in the following location: Policy > Policy Sets > Default > Authorization Policy.

You must ensure that the endpoint profiling policies are either standalone policies (not a parent to other endpoint profiling policies), or their parent policies of the endpoint profiling policies are not disabled.
Profiler Feed Service

Profiler conditions, exception actions, and NMAP scan actions are classified as Cisco-provided or administrator-created (see the System Type attribute). Also, the endpoint profiling policies are classified as Cisco provided, administrator created, or administrator modified (see the System Type attribute).

You can perform different operations on the profiler conditions, exception actions, NMAP scan actions, and endpoint profiling policies depending on the System Type attribute. You cannot edit or delete Cisco-provided conditions, exception actions, and nmap scan actions. Endpoint policies that are provided by Cisco cannot be deleted. When policies are edited, they are considered as administrator-modified. When administrator-modified policies are deleted, they are replaced by the up-to-date version of the Cisco-provided policy that it was based on.

You can retrieve new and updated endpoint profiling policies and the updated OUI database as a feed from a designated Cisco feed server through a subscription in to Cisco ISE. You can also receive e-mail notifications to the e-mail address as an administrator of Cisco ISE that you have configured for applied, success, and failure messages. You can also provide additional subscriber information to receive notifications. You can send the subscriber information back to Cisco for maintaining the records and they are treated as privileged and confidential.

Cisco ISE downloads the feed service policies and OUI database updates every day at 1:00 A.M of the local Cisco ISE server time zone. Cisco ISE automatically applies these downloaded feed server policies, which also stores the set of changes so that you can revert these changes back to the previous state. When you revert from the set of changes that you last applied, endpoint profiling policies that are newly added are removed and endpoint profiling policies that are updated are reverted to the previous state. In addition, the profiler feed service is automatically disabled.

You can also update the feed services manually in offline mode. You can download the updates manually by using this option if you cannot connect your ISE deployments to Cisco feed service.

When the updates occur, only the Cisco provided profiling policies and the endpoint profiling policies which were modified by the previous update, are updated. Cisco provided disabled profiling policies are also updated but they remain disabled. Administrator Created or Administrator Modified profiling policies are not overwritten. If you want to revert any Administrator Modified endpoint profiling policy to any Cisco Provided endpoint profiling policy, then you must delete or revert the Administrator Modified endpoint profiling policy to the previous Cisco Provided endpoint profiling policy.

---

Note

Updates from the Feed Service are not allowed after the license goes Out of Compliance (OOC) for 45 days within a 60-day window period. The license is out of compliance when it has expired, or when the usage exceeds the allowed number of sessions.

---

OUI Feed Service

The designated Cisco feed server downloads the updated OUI database from http://standards.ieee.org/develop/regauth/oui/oui.txt, which is the list of vendors associated to the MAC OUI. The updated OUI database is available for any ISE deployment as a feed that Cisco ISE downloads to its own database. Cisco ISE updates endpoints and then starts reprofiling endpoints.

The designated Cisco feed server is located at https://ise.cisco.com:8443/feedserver/. If you have any issues accessing the service, ensure that your network security components (like a firewall or proxy server, for example) allow direct access to this URL.
Configure Profiler Feed Service

The Profiler Feed Service retrieves new and updated endpoint profiling policies and MAC OUI database updates from the Cisco Feed server. If the Feed Service is unavailable or other errors have occurred, it is reported in the Operations Audit report.

You can configure Cisco ISE to send the feed service usage report back to Cisco, which sends the following information to Cisco:

- Hostname - Cisco ISE hostname
- MaxCount - Total number of endpoints
- ProfiledCount - Profiled endpoints count
- UnknownCount - Unknown endpoints count
- MatchSystemProfilesCount - Cisco Provided profiles count
- UserCreatedProfiles - User created profiles count

You can change the CoA type in a Cisco-provided profiling policy. When the feed service updates that policy, the CoA type will not be changed, but the rest of that policy's attributes will be still be updated.

Before you begin

The Profiler feed service can only be configured from the Cisco ISE Admin portal in a distributed deployment or in a standalone ISE node.

Set up a Simple Mail Transfer Protocol (SMTP) server if you plan to send e-mail notifications from the Admin portal about feed updates (Administration > System > Settings).

To update the Feed Services online:

Step 1 Choose Administration > Certificates > Trusted Certificates, and check if Verisign Class 3 Public Primary Certification Authority and Verisign Class 3 Server CA - G3 are enabled.

Step 2 Choose Work Centers > Profiler > Feeds. You can also access the option in the Administration > FeedService > Profiler page.

Step 3 Click the Online Subscription Update tab.

Step 4 Click the Test Feed Service Connection button to verify that there is a connection to the Cisco Feed Service, and that the certificate is valid.

Step 5 Check the Enable Online Subscription Update check box.

Step 6 Enter time in HH:MM format (local time zone of the Cisco ISE server). By default, Cisco ISE feed service is scheduled at 1.00 AM every day.

Step 7 Check the Notify administrator when download occurs check box and enter your e-mail address in the Administrator email address text box. Check the Provide Cisco anonymous information to help improve profiling accuracy check box, if you want to allow Cisco ISE to collect non-sensitive information (that will be used to provide better services and additional features in forthcoming releases).

Step 8 Click Save.

Step 9 Click Update Now.

Instructs Cisco ISE to contact Cisco feed server for new and updated profiles created since the last feed service update. This re-profiles all endpoints in the system, which may cause an increase the load on the system. Due to updated endpoint
profiling policies, there may be changes in the authorization policy for some endpoints that are currently connected to Cisco ISE.

The Update Now button is disabled when you update new and updated profiles created since the last feed service and enabled only after the download is completed. You must navigate away from the profiler feed service Configuration page and return to this page.

---

**Related Topics**

Configure Profiler Feed Services Offline, on page 718

---

**Configure Profiler Feed Services Offline**

You can update the feed services offline when Cisco ISE is not directly connected to the Cisco feed server. You can download the offline update package from the Cisco feed server and upload it to Cisco ISE using the offline feed update. You can also set email notifications about new policies that are added to the feed server.

Configuring the profiler feed services offline involves the following tasks:

1. Download Offline Update Package
2. Apply Offline Feed Updates

---

**Download Offline Update Package**

To download offline update package:

---

**Step 1**

Choose Work Centers > Profiler > Feeds.

You can also access the option in the Administration > FeedService > Profiler page.

**Step 2**

Click the Offline Manual Update tab.

**Step 3**

Click Download Updated Profile Policies link. You will be redirected to Feed Service Partner Portal.

You can also go to https://ise.cisco.com/partner/ from your browser, to go to the feed service partner portal directly.

**Step 4**

If you are a first time user, accept the terms and agreements.

An email will be triggered to Feed Services administrator to approve your request. Upon approval, you will receive a confirmation email.

**Step 5**

Login to the partner portal using your Cisco.com credentials.

**Step 6**

Choose Offline Feed > Download Package .

**Step 7**

Click Generate Package.

**Step 8**

Click the Click to View the Offline Update Package contents link to view all the profiles and OUIs that are included in the generated package.

- The policies under Feed Profiler 1 and Feed OUI will be downloaded to all versions of Cisco ISE.
- The policies under Feed Profiler 2 will be downloaded only to Cisco ISE Release 1.3 and later.
- The policies under Feed Profiler 3 will be downloaded only to Cisco ISE Release 2.1 and later.

**Step 9**

Click Download Package and save the file to your local system.

You can upload the saved file to Cisco ISE server to apply the feed updates in the downloaded package.
Apply Offline Feed Updates

To apply the downloaded offline feed updates:

**Before you begin**

You must have downloaded the offline update package before applying the feed updates.

**Step 1** Choose **Work Centers** > **Profiler** > **Feeds**.
You can also access the option in the **Administration** > **FeedService** > **Profiler** page.

**Step 2** Click the **Offline Manual Update** tab.

**Step 3** Click **Browse** and choose the downloaded profiler feed package.

**Step 4** Click **Apply Update**.

**Configure Email Notifications for Profile and OUI Updates**

You can configure your email address to receive notifications on profile and OUI updates.

To configure email notifications:

**Step 1** Perform **Step 1** through **Step 5** in the **Download Offline Update Package** section to go to the Feed Service Partner Portal.

**Step 2** Choose **Offline Feed** > **Email Preferences**.

**Step 3** Check the **Enable Notifications** checkbox to receive notifications.

**Step 4** Choose the number of days from the **days** drop-down list to set the frequency in which you want to receive the notifications on new updates.

**Step 5** Enter the e-mail address/addresses and click **Save**.

**Undo Feed Updates**

You can revert endpoint profiling policies that were updated in the previous update and remove endpoint profiling policies and OUIs that are newly added through the previous update of the profiler feed service.

An endpoint profiling policy, if modified after an update from the feed server is not changed in the system.

**Step 1** Choose **Work Centers** > **Profiler** > **Feeds**.

**Step 2** Click **Go to Update Report Page** if you want to view the configuration changes made in the Change Configuration Audit report.

**Step 3** Click **Undo Latest**.
Profiler Reports

Cisco ISE provides you with various reports on endpoint profiling, and troubleshooting tools that you can use to manage your network. You can generate reports for historical as well as current data. You may be able to drill down on a part of the report to view more details. For large reports, you can also schedule reports and download them in various formats.

You can run the following reports for endpoints from Operations > Reports > Endpoints and Users:

- Endpoint Session History
- Profiled Endpoint Summary
- Endpoint Profile Changes
- Top Authorizations by Endpoint
- Registered Endpoints

Detect Anomalous Behavior of Endpoints

Cisco ISE protects your network from the illegitimate use of a MAC address. ISE detects the endpoints involved in MAC address spoofing and allows you to restrict the permission of the suspicious endpoints.

The following are the two options in the profiler configuration page for Anomalous Behavior:

- Enable Anomalous Behavior Detection
- Enable Anomalous Behavior Enforcement

If you enable Anomalous Behavior detection, Cisco ISE probes for data, and checks for any contradiction to the existing data with respect to changes in attributes related to NAS-Port-Type, DHCP Class Identifier, and Endpoint Policy. If so, an attribute called AnomalousBehavior set to true is added to the endpoint which helps you to filter and view the endpoints in the Visibility Context page. Audit logs are also generated for the respective MAC address.

When anomalous behavior detection is enabled, Cisco ISE checks if the following attributes of existing endpoints have changed:

1. Port-Type—Determines if the access method of an endpoint has changed. For example, if the same MAC address that connected via Wired Dot1x has been used for Wireless Dot1x and visa-versa.

2. DHCP Class Identifier—Determines whether the type of client or vendor of an endpoint has changed. This only applies when DHCP Class identifier attribute is populated with a certain value and is then changed to another value. If an endpoint is configured with a static IP, the DHCP Class Identifier attribute is empty in Cisco ISE. Later on, if another device spoofs the MAC address of this endpoint and uses DHCP, the Class Identifier changes from an empty value to a specific string. This will not trigger anomalous behavior detection.

3. Endpoint Policy—Determines if there are significant profile changes. For example, if the profile of an endpoint changes from a “Phone” or “Printer” to a “Workstation”.
If you enable Anomalous Behavior Enforcement, a CoA is issued upon detection of the anomalous Behavior, which can be used to re-authorize the suspicious endpoints, based on the authorization rules configured in the Profiler Configuration page.

To set the authorization policy rules for endpoints with anomalous Behavior, see .

**Set Authorization Policy Rules for Endpoints with Anomalous Behavior**

This task configures the action taken against any endpoint with anomalous Behavior by setting the corresponding rules on the Authorization Policy page.

**Step 1** Choose **Policy > Policy Sets**.

**Step 2** Click the arrow icon from the **View** column corresponding to the Default Policy to open the Set view screen and view and manage the default authorization policy.

**Step 3** From the **Actions** column on any row, click the cog icon and then from the drop-down list, insert a new authorization rule by selecting any of the insert or duplicate options, as necessary.

A new row appears in the Policy Sets table.

**Step 4** Enter the Rule Name.

**Step 5** From the **Conditions** column, click the (+) symbol.

**Step 6** Create the required conditions on the **Conditions Studio Page**. In the **Editor** section, click the **Click To Add an Attribute** text box, and select the required Dictionary and Attribute (for example, Endpoints.AnomalousBehaviorEqualsTrue).

You can also drag and drop a Library condition to the **Click To Add An Attribute** text box.

**Step 7** Click **Use** to set the authorization policy rules for endpoints with anomalous behavior.

**Step 8** Click **Done**.

---

**View Endpoints with Anomalous Behavior**

You can view the endpoints with anomalous behavior by using any of the following options:

- Click Anomalous Behavior from **Home > Summary > Metrics**. This action opens a new tab with Anomalous Behaviour column in the lower pane of the page.

- Choose **Context Visibility > Endpoints > Endpoint Classification**. You can view the Anomalous Behaviour column in the lower pane of the page.

- You can create a new Anomalous Behavior column in Authentication view or Compromised Endpoints view in the Context Visibility page as explained in the following steps:

**Step 1** Choose **Context Visibility > Endpoints > Authentication** or **Context Visibility > Endpoints > Compromised Endpoints**.

**Step 2** Click the Settings icon in the lower pane of the page and check **Anomalous Behavior** checkbox.

**Step 3** Click **Go**.

You can view the Anomalous Behavior column in the Authentication or Compromised Endpoints View.
Configure Client Provisioning

Configure Client Provisioning in Cisco ISE

Enable client provisioning to allow users to download client provisioning resources and configure agent profiles. You can configure agent profiles for Windows clients, Mac OS X clients, and native supplicant profiles for personal devices. If you disable client provisioning, users attempting to access the network will receive a warning message indicating that they are not able to download client provisioning resources.

Before you begin

If you are using a proxy, and hosting client provisioning resources on a remote system, verify that the proxy allows clients to access that remote location.
Step 1  Choose Administration > System > Settings > Client Provisioning.

Step 2  From the Enable Provisioning drop-down list, choose Enable or Disable.

Step 3  From the Enable Automatic Download drop-down list, choose Enable.

Feed downloads include all the available client provisioning resources. Some of these resources may not be pertinent to your deployment. Cisco recommends manually downloading resources whenever possible instead of setting this option.

Step 4  Update Feed URL—Specify the URL where Cisco ISE searches for system updates in the Update Feed URL text box. For example, the default URL for downloading client-provisioning resources is https://www.cisco.com/web/secure/pmbu/provisioning-update.xml.

If your network restricts URL-redirection functions (via a proxy server, for example) and you are experiencing difficulty accessing the default URL, try also pointing your Cisco ISE to the following URL: https://www.perfigo.com/ise/provisioning-update.xml.

Step 5  Native Supplicant Provisioning Policy Unavailable—When there is no client provisioning resource for a device, decide here how to proceed in the flow:

• Allow Network Access—Users are allowed to register their device on the network without having to install and launch the native supplicant wizard.

• Apply Defined Authorization Policy—Users must try to access the Cisco ISE network via standard authentication and authorization policy application (outside of the native supplicant provisioning process). If you enable this option, the user device goes through standard registration according to any client-provisioning policy applied to the user’s ID. If the user’s device requires a certificate to access the Cisco ISE network, you must also provide detailed instructions to the user describing how to obtain and apply a valid certificate using the customizable user-facing text fields, as described in the “Adding a Custom Language Template” section in the Chapter 15, Setting up and Customizing End_User Web Portals.

Step 6  Click Save.

What to do next
Configure client provisioning resource policies.

Client Provisioning Resources

Client provisioning resources are downloaded to endpoints after the endpoint connects to the network. Client provisioning resources consist of compliance and posture agents for desktops, and native supplicant profiles for phones and tablets. Client provisioning policies assign these provisioning resources to endpoints to start a network session.

Client provisioning resources are listed on Policy Elements > Results > Client Provisioning > Resources. The following resource types can be added to the list by clicking the Add button:

• Agent resources from Cisco Site—Select the NAC, AnyConnect, and Supplicant Provisioning wizards you want to make available for client provisioning policies. Cisco periodically updates this list of resources, adding new ones and updating existing ones. You can also set up ISE to download all the Cisco resources and resource updates automatically, see Configure Client Provisioning in Cisco ISE, on page 737 for more information.
• **Agent resources from local disk**—Select resources on your PC that you want to upload to ISE, see Add Cisco Provided Client Provisioning Resources from a Local Machine, on page 740.

• **AnyConnect Configuration**—Select the AnyConnect PC clients that you want to make available for client provisioning. See Create AnyConnect Configuration for more information.

• **Native Supplicant Profile**—Configure a supplicant profile for phones and tablets that contains settings for your network. For more information, see Create Native Supplicant Profiles.

• **NAC Agent or AnyConnect ISE Posture Profile**—Configure the NAC agent and AnyConnect ISE Posture here when you don't want to create and distribute agent XML profiles. For more information about the AnyConnect ISE Posture agent and ISE Posture Profile Editor, see the AnyConnect Administrators Guide for your version of AnyConnect https://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-installation-and-configuration-guides-list.html.

After creating client provisioning resources, create client provisioning policies that apply the client provisioning resources to the endpoints. See Configure Client Provisioning Resource Policies, on page 767.

**Related Topics**
- Configure Client Provisioning in Cisco ISE, on page 737
- Add Client Provisioning Resources from Cisco, on page 739
- Download Client Provisioning Resources Automatically
- Add Cisco Provided Client Provisioning Resources from a Local Machine, on page 740
- Add Customer Created Resources for AnyConnect from a Local Machine, on page 740

### Add Client Provisioning Resources from Cisco

You can add client provisioning resources from Cisco.com for AnyConnect and Cisco NAC Agent for Windows and MAC OS x clients, and Cisco Web agent. Depending on the resources that you select and available network bandwidth, Cisco ISE can take a few seconds or even a few minutes to download client provisioning resources to Cisco ISE.

**Before you begin**

- Ensure that you have the correct proxy settings configured in Cisco ISE.
- Enable client provisioning in Cisco ISE.

**Step 1** Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.

**Step 2** Choose **Add > Agent resources from Cisco site**.

**Step 3** Select one or more required client provisioning resources from the list available in the Download Remote Resources dialog box.

**Step 4** Click **Save**.

**What to do next**

After you have successfully added client provisioning resources to Cisco ISE, you can begin to configure client provisioning resource policies.
Add Cisco Provided Client Provisioning Resources from a Local Machine

You can add client provisioning resources from the local disk, which you might have previously downloaded from Cisco.

Before you begin

Be sure to upload only current, supported resources to Cisco ISE. Older, unsupported resources (older versions of the Cisco NAC Agent, for example) will likely cause serious issues for client access.

If you are downloading the resource files manually from the Cisco.com, refer to “Cisco ISE Offline Updates” section in the Release Notes.

| Step 1 | Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**. |
| Step 2 | Choose **Add > Agent resources from local disk**. |
| Step 3 | Choose **Cisco Provided Packages** from the Category drop-down. |
| Step 4 | Click **Browse** to the directory on your local machine where the resource file that you want to download to Cisco ISE resides. You can add AnyConnect, Cisco NAC Agent, and Cisco Web Agent resources that you have previously downloaded from Cisco site in your local machine. |
| Step 5 | Click **Submit**. |

What to do next

After you have successfully added client provisioning resources to Cisco ISE, you can begin to configure client provisioning resource policies.

Add Customer Created Resources for AnyConnect from a Local Machine

Add customer created resources like AnyConnect customization and localization packages and AnyConnect profiles from the local machine to Cisco ISE.

Before you begin

Ensure that customer created resources for AnyConnect are zipped files and available in your local disk.

| Step 1 | Choose **Policy > Policy Elements > Results > Client provisioning > Resources**. |
| Step 2 | Click **Add**. |
| Step 3 | Choose **Agent Resources from local disk**. |
Step 4   Choose **Customer Created Packages** from the Category drop-down.

Step 5   Enter the name and description for AnyConnect resources.

Step 6   Click **Browse** to the directory on your local machine where the resource file that you want to download to Cisco ISE resides.

Step 7   Choose the following AnyConnect resources to upload to Cisco ISE:

- AnyConnect customization bundle
- AnyConnect localization bundle
- AnyConnect profile
- Advanced Malware Protection (AMP) Enabler Profile

Step 8   Click **Submit**.

The Uploaded AnyConnect Resources table displays AnyConnect resources that you add to Cisco ISE.

---

**What to do next**

Create AnyConnect agent profile

---

**Create Native Supplicant Profiles**

You can create native supplicant profiles to enable users to bring their own devices into the Cisco ISE network. When the user signs in, Cisco ISE uses the profile that you associated with that user’s authorization requirements to choose the necessary supplicant provisioning wizard. The wizard runs and sets up the user’s personal device to access the network.

---

**Note**

The provisioning wizard only configures interfaces which are active. Because of this, users with Wired and Wireless connections will not be provisioned for both interfaces, unless they are both active.

---

**Before you begin**

- If you intend to use a TLS device protocol for remote device registration, set up at least one Simple Certificate Enrollment Protocol (SCEP) profile.

- Open up TCP port 8909 and UDP port 8909 to enable installation of Cisco NAC Agent, Cisco NAC Web Agent, and supplicant provisioning wizard. For more information about port usage, see the “Cisco ISE Appliance Ports Reference” appendix in the *Cisco Identity Services Engine Hardware Installation Guide*.

---

**Step 1**   Choose **Policy > Policy Elements > Results > Client Provisioning > Resources**.

**Step 2**   Choose **Add > Native Supplicant Profile**.

**Step 3**   Create a profile, using the descriptions described in [Native Supplicant Profile Settings, on page 742](#).
What to do next

Enable self-provisioning capabilities that allow employees to directly connect their personal devices to the network, as described in the Support for multiple Guest Portals section.

Native Supplicant Profile Settings

When you choose Policy > Policy Elements > Results > Client Provisioning Resources, and add a Native Supplicant Profile, you will see the following settings.

• **Name**—Name of the native supplicant profile that you are creating, and select which operating system(s) this profile should apply to. Each profile defines settings for a network connection that ISE will apply to the client's native supplicant.

Wireless Profile(s)

Configure one or more Wireless profiles, one for each SSID that you want to make available to the client.

• **SSID Name**—Name of the SSID that the client will connect to.

• **Proxy Auto-Config File URL**—If the client will connect to a proxy to get the network configuration for its supplicant, enter the URL to that proxy server.

• **Proxy Host/IP**

• **Proxy Port**

• **Security**—Configure the client to use WPA or WPA2.

• **Allowed Protocol**—Configure which protocol the client should use to connect to the authentication server; PEAP or EAP-TLS.

• **Certificate Template**—For TLS, choose one of the certificate templates defined on Administration > System Certificates > Certificate Authority > Certificate Templates.

Optional Settings are described in the section Optional Settings - for Windows.

iOS Settings

• **Enable if target network is hidden**

Wired Profile

• **Allowed Protocol**—Configure which protocol the client should use to connect to the authentication server; PEAP or EAP-TLS.

• **Certificate Template**—For TLS, choose one of the certificate templates that defined on Administration System Certificates Certificate Authority Certificate Templates

Optional Settings - for Windows

If you expand Optional, the following fields are also available for Windows clients.

• **Authentication Mode**—Decide whether to use User, Machine or both as credentials for authorization.
• **Automatically use logon name and password (and domain if any)**—If you selected User for authentication mode, use the logon and password to without prompting the user, if that information is available.

• **Enable Fast Reconnect**—Allow a PEAP session to resume without checking user credentials when the session resume feature is enabled in the PEAP protocol options, which is configured on **Administration > System > Settings > Protocols > PEAP**.

• **Enable Quarantine Checks**—Check if the client has been quarantined.

• **Disconnect if server does not present cryptobinding TLV**—Disconnect if cryptobinding TLV is not supported for the network connection.

• **Do not prompt user to authorize new servers or trusted certification authorities**—Automatically accept user certificates; do not prompt the user.

• **Connect even if the network is not broadcasting its name (SSID)**—For Wireless profiles only.

## Client Provisioning Without URL Redirection for Different Networks

Client provisioning without URL redirection is required when the third party NAC does not support CoA. You can perform client provisioning with and without URL redirection.

### Note

For client provisioning with URL redirection, if the client machine has proxy settings configured, ensure that you add Cisco ISE to the list of exceptions in the browser settings. This setting is applicable for all flows, BYOD, MDM, Guest, and Posture that use URL redirection. For example, on Windows machines, do the following:

1. From Control Panel, click **Internet Properties**.
2. Select the **Connections** tab.
3. Click **LAN settings**.
4. Click **Advanced** from the Proxy server area.
5. Enter the IP addresses of the Cisco ISE nodes in the **Exceptions** box.
6. Click **OK**.

Given below are the steps you perform to provision an endpoint without redirection for different networks.

**Dot1X EAP-TLS**

1. Connect the Cisco ISE network with provisioned certification.
2. Open a browser window and type in the provisioning URL: provisioning.cisco.com.
3. Log into the CP portal via internal user, AD, LDAP, or SAML.
   AnyConnect performs posture. The endpoint moves to the right network based on posture compliance.
Dot1X PEAP

1. Connect the Cisco ISE network with User Name and Password through NSP
2. Open a browser window and type in the provisioning URL: provisioning.cisco.com.
3. Log into the CP portal via internal user, AD, LDAP, or SAML.
   AnyConnect performs posture. The endpoint moves to the right network based on posture compliance.

MAB (Wired Networks)

1. Connect the Cisco ISE network.
2. Open a browser window and type in the provisioning URL: provisioning.cisco.com.
3. Log into the CP portal via internal user, AD, LDAP, or SAML.
   AnyConnect performs posture. The endpoint moves to the right network based on posture compliance.

MAB (Wireless Networks)

1. Connect the Cisco ISE network
2. Open a browser window and type in the provisioning URL: provisioning.cisco.com.
3. Log into the CP portal via internal user, AD, LDAP, or SAML.
   AnyConnect performs posture. Posture starts for wireless 802.1X only.

AMP Enabler Profile Settings

The following table describes the fields in the Advanced Malware Protection (AMP) Enabler Profile page. The navigation path is: Policy > Policy Elements > Results > Client Provisioning > Resources.

Click the Add drop-down arrow and select the AMP Enabler Profile.

**Table 64: AMP Enabler Profile Page**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the AMP enabler profile that you want to create.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the AMP enabler profile.</td>
</tr>
</tbody>
</table>
Create an AMP Enabler Profile Using the Embedded Profile Editor

You can create the AMP enabler profile using the ISE embedded profile editor or the standalone editor. To create the AMP enable profile using the ISE embedded profile editor:

**Before you begin**
- Download the AMP for Endpoint software from the SOURCEfire portal and host it on a local server.
- Import the certificate of the server that hosts the AMP for endpoint software to the ISE certificate store by navigating to Administration > Certificates > Trusted Certificates.
- Ensure that the AMP Enabler options are selected in the AnyConnect Module Selection and Profile Selection sections in the AnyConnect Configuration page (Policy > Policy Elements > Results > Client provisioning > Resources > Add > AnyConnect Configuration > Select AnyConnect Package).
- You must log in to the SOURCEfire portal, create policies for endpoint groups, and download the AMP for endpoint software. The software comes preconfigured with the policies that you have chosen.

---

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
</table>
| Install AMP Enabler     | • **Windows Installer**—Specify the URL of the local server that hosts the AMP for Windows OS software. The AnyConnect module uses this URL to download the .exe file to the endpoint. The file size is approximately 25 MB.  
                          • **Mac Installer**—Specify the URL of the local server that hosts the AMP for Mac OSX software. The AnyConnect module uses this URL to download the .pkg file to the endpoint. The file size is approximately 6 MB.  
                          The Check button communicates with the server to verify if the URL is valid. If the URL is valid, a "File found" message is displayed or else an error message is displayed. |
| Uninstall AMP Enabler   | Uninstalls the AMP for endpoint software from the endpoint.                      |
| Add to Start Menu       | Adds a shortcut for the AMP for endpoint software in the Start menu of the endpoint, after the AMP for endpoint software is installed on the endpoint. |
| Add to Desktop          | Adds an icon for the AMP for endpoint software on the desktop of the endpoint, after the AMP for endpoint software is installed on the endpoint. |
| Add to Context Menu     | Adds the Scan Now option in the right-click context menu of the endpoint, after the AMP for endpoint software is installed on the endpoint. |
must download two images, namely, the redistributable version of the AMP for endpoint software for Windows OS and AMP for endpoint software for Mac OSx. The downloaded software is hosted on a server that is accessible from the enterprise network.

Step 1 Choose Policy > Policy Elements > Results > Client Provision > Resources.
Step 2 Click the Add drop-down.
Step 3 Choose AMP Enabler Profile to create a new AMP enabler profile.
Step 4 Enter the appropriate values in the fields.
Step 5 Click Submit to save the profile in the Resources page.

---

Create an AMP Enabler Profile Using the Standalone Editor

To create an AMP enabler profile using the AnyConnect standalone editor.

Before you begin

You can create an AMP enabler profile by uploading the XML format of the profile using the AnyConnect 4.1 standalone editor.

- Download the AnyConnect standalone profile editor for Windows and Mac OS from Cisco.com.
- Launch the standalone profile editor and enter the fields as specified in the AMP Enabler Profile Settings.
- Save the profile as an XML file in your local disk.
- Ensure that the AMP Enabler options are selected in the AnyConnect Module Selection and Profile Selection sections in the AnyConnect Configuration page (Policy > Policy Elements > Results > Client provisioning > Resources > Add > AnyConnect Configuration > Select AnyConnect Package).

---

Step 1 Choose Policy > Policy Elements > Results > Client provisioning > Resources.
Step 2 Click Add.
Step 3 Choose Agent resources from local disk.
Step 4 Choose Customer Created Packages from the Category drop-down.
Step 5 Choose AMP Enabler Profile from the Type drop-down.
Step 6 Enter a Name and Description.
Step 7 Click Browse and select the saved profile (XML file) from the local disk. The following example shows a customized install file.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<FAConfiguration>
<Install>
<WindowsConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</WindowsConnectorLocation>
<MacConnectorLocation>
https://fa_webserver/ACFA_Mac_FireAMPSetup.exe
</MacConnectorLocation>
</Install>
</FAProfile>
```
The following example shows a customized uninstall file.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <FAConfiguration>
    <Uninstall />
  </FAConfiguration>
</FAProfile>
```

Step 8  Click Submit.

The newly created AMP Enabler profile is displayed in the Resources page.

### Troubleshoot Common AMP Enabler Installation Errors

When you enter the SOURCEfire URL in the Windows or MAC Installer text box and click Check, you might encounter any of the following errors:

- **Error Message:** The certificate for the server containing the Mac/Windows installer file is not trusted by ISE. Add a trust certificate to Administration > Certificates > Trusted Certificates.

  This error message appears if you have not imported the SOURCEfire trusted certificate into the Cisco ISE certificate store. Obtain a SOURCEfire trusted certificate and import it into the Cisco ISE trusted certificate store (Administration > Certificates > Trusted Certificates).

- **Error Message:** The installer file is not found at this location, this may be due to a connection issue. Enter a valid path in the Installer text box or check your connection.

  This error message appears when the server hosting the AMP for Endpoint software is down or if there is a typographic error in the Windows Installer or MAC Installer text box.

- **Error Message:** The Windows/Mac installer text box does not contain a valid URL.

  This error message appears when you enter a syntactically incorrect URL format.

### Cisco ISE Support for Onboarding Chromebook Devices

Chromebook devices are managed devices (managed by the Google domain), unlike other devices (Apple, Windows, Android) and have limited onboarding support. Cisco ISE supports the onboarding of Chromebook devices on a network. Onboarding refers to the process of delivering the required settings and files to an endpoint such that it is able to connect securely to a network after authenticating with Cisco ISE. This process includes certificate provisioning and/or native supplicant provisioning. However, in Chromebook devices, you can only perform certificate provisioning. Native supplicant provisioning is done via the Google Admin Console.

Unmanaged Chromebook devices cannot be onboarded to a secure network.
The entities involved in the Chromebook onboarding process are the:

- Google Administrator
- ISE Administrator
- Chromebook User/Device
- Google Admin Console (Managed by the Google Administrator)

The Google administrator:

- Secures the following licenses:
  1. Google Apps Administrator license for the Google Admin Console configuration—URL: https://admin.google.com. The Google Admin Console enables an administrator to manage Google services for people in an organization.
  2. Chromebook device management license—URL: https://support.google.com/chrome/a/answer/2717664?hl=en. A Chromebook device management license is used to configure settings and enforce policies for a specific Chromebook device. It gives the Google Administrator access to device settings to control user access, customize features, configure network access, and more.
- Facilitates provisioning and enrolling of Chromebook devices with a Google device license.
- Manages Chromebook devices through the Google Admin Console.
- Sets up and manages the Wi-Fi network configuration for each Chromebook user.
- Manages the Chromebook devices by configuring applications and forced extensions to be installed on the Chromebook device. Onboarding the Chromebook device requires the Cisco Network Setup Assistant extensions to be installed in the Chromebook device. This allows the Chromebook device to connect to Cisco ISE and install the ISE certificate. The extension is forcibly installed because the action of certificate installation is allowed only for managed devices.
- Ensures that the Cisco ISE certificates are installed in the Google Admin Console to provide server validation and secure connection. The Google administrator decides whether a certificate should be generated for a device or a user. Cisco ISE provides options to:
  - Generate the certificate for a single user who does not share the Chromebook device.
  - Generate a certificate for a Chromebook device that is shared by multiple users. Refer to Step 5 in the Configure the Network and Force Extensions in the Google Admin Console section for the required additional configuration.

The Google Administrator installs the ISE server certificate so that ISE is trusted to perform the certificate provisioning on the Chromebook device and also to allow EAP-TLS certificate-based authentication. Google Chrome version 37 and higher supports certificate-based authentication for Chromebook devices. The Google administrator needs to load the ISE provisioning application in the Google Admin Console and make it available to the Chromebook devices to get the certificate from ISE.

- Ensures that the recommended Google host names are white listed in the ACL definition list configured in the WLC for SSL secure connections. Refer to the recommended host name white list in the Google Support page.

The ISE Administrator:

- Defines the native supplicant profile for the Chromebook OS that includes the certificate template structure.
• Creates the necessary authorization rules and client provisioning policies in Cisco ISE for Chromebook users.

The Chromebook User:

• Wipes out the Chromebook device and enrolls it to the Google domain to secure the enforced policy that was defined by the Google administrator.
• Receives the Chromebook device policies and the Cisco Network Setup Assistant forced extension installed by the Google Admin Console.
• Connects to the provisioned SSID, as defined by the Google administrator, opens the browser, displays the BYOD pages, and starts the onboarding process.
• The Cisco Network Setup Assistant installs a client certificate in the Chromebook device, which allows the device to perform EAP-TLS certificate-based authentication.

The Google Admin Console:

The Google Admin Console supports Chromebook device management and allows configuring a secure network and pushing Cisco Network Setup Assistant certificate management extensions to the Chromebook. The extension sends an SCEP request to Cisco ISE and installs the client certificate to allow secure connection and access to the network.

Best Practices for Using Chromebook Device in a Shared Environment

When a Chromebook device is used in a shared environment, such as schools and libraries, the Chromebook device is shared by different users. Some of the best practices that Cisco recommends include:

• When onboarding a Chromebook device with a specific user (student or professor) name, the user's name will be populated in the Common Name (CN) in the Subject field of the certificate. Also, the shared Chromebook is listed in the My Devices portal under that specific user. Therefore, it is recommended for shared devices to use a shared credential when onboarding, so that devices show up only under the specific user's My Devices portal listing. The shared account can be administered by the administrator or professor as a separate account to control shared devices.

• The ISE administrator can create a custom certificate template for shared Chromebook devices and use it in the policy. For example, instead of using the standard certificate template that matches the Subject-Common Name (CN) value, you can specify a Name (for example, chrome-shared-grp1) in the certificate and the same name can be assigned to the Chromebook device. A policy can be designed to match the name to allow or deny access to a Chromebook device.

• The ISE administrator can create an endpoint group with all the Chromebook devices’ MAC addresses that needs to go through Chromebook onboarding (devices for which access need to be restricted). The authorization rule should call this out along with device type Chromebook—this would allow access to be redirected to the NSP.

Chromebook Onboarding Process

The Chromebook onboarding process involves a series of steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure the Network and Force Extensions in the Google Admin Console.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Configure ISE for Chromebook Onboarding.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Wipe a Chromebook Device.</td>
</tr>
</tbody>
</table>
Configure the Network and Force Extensions in the Google Admin Console

The following steps are performed by the Google administrator.

**Step 1** Log in to the Google Admin Console.
- a) Enter the following URL: https://admin.google.com in the browser.
- b) Enter the required username and password.
- c) In the Welcome to Admin Console page, click Device Management.
- d) In the Device Management page, click Network.

**Step 2** Set up the Wi-Fi network for managed devices.
- a) In the Networks page, click Wi-Fi.
- b) Click Add Wi-Fi to add the required SSIDs. Refer to Google Admin Console - Wi-Fi Network Settings page for more information.
  
  For MAB flows, create two SSIDs, one for the open network and the other for certificate authentication. When connecting to the open network, Cisco ISE ACLs redirect the user to the credentialed guest portal and after authentication redirects to the BYOD portal.
- c) Click Add.

**Step 3** Create the forced extensions.
- a) In the Device Management page, in the Device Settings area, click Chrome Management.
- b) Click User Settings.
- c) Scroll down, and in the Apps and Extensions section, in the Force-Installed Apps and Extensions option, click Manage Force-Installed Apps.

**Step 4** Install the forced extensions.
- a) In the Force-Installed Apps and Extensions page, click Chrome Web Store.
- b) In the Search text box type "Cisco Network Setup Assistant" to locate the extension.
  
  The forced Cisco Network Setup Assistant extension of the Chromebook device requests the certificate from Cisco ISE and installs the ISE certificate on the Chromebook device. The extension must be configured as force-installed because the action of certificate installation is allowed only for managed devices. If the extension is not installed in the Chromebook during the enrollment process, the Cisco ISE certificate cannot be installed.
  
  Refer to the Cisco ISE Internationalization and Localization topic for more information on the languages supported by extensions.
- c) Click Add to force install apps.
- d) Click Save.

**Step 5** (Optional) Define the configuration file to install a certificate in a Chromebook device that is shared by multiple users.
- a) Copy and paste the following code in a Notepad file and save it to your local disk.

```json
{
  "certType": {
    "value": "system"
  }
```
b) Choose Device Management > Chromebook Management > App Management.

c) Click the Cisco Network Setup Assistant extension.

d) Click User Settings and choose your domain.

e) Click Upload Configuration File and choose the .txt file that you have saved in your local disk.

Note For the Cisco Network Setup Assistant to create a certificate for a device that is shared by multiple users, you must add the Notepad file in the Google Admin Console. Otherwise, the Cisco NSA creates a certificate for a single user.

f) Click Save.

Step 6 (Optional) Install a certificate for a single user who does not share the Chromebook device.

a) Choose Device Management > Network > Certificates.

b) In the Certificates section, click Add Certificate and upload the Cisco ISE certificate file.

What to do next
Configure ISE for Chromebook Onboarding.

Configure ISE for Chromebook Onboarding

Before you begin
The ISE administrator must create the required policy in the Policy > Policy Sets page.

Given below is an example of an authorization policy:


The CompliantNetworkAccess is an authorization result configured in the Policy > Policy Elements > Results > Authorization > Authorization Profiles page.

Step 1 Configure the Native Supplicant Profile (NSP) on Cisco ISE.

a) Choose Policy > Policy Elements > Results.

b) Click Client Provisioning > Resources.

The Chromebook device is displayed in the Client Provisioning page for a fresh Cisco ISE installation. However, for upgrade, you should download posture updates from the Administration > System > Settings > Posture > Updates page.

c) Click Add > Native Supplicant Profile.

d) Enter the Name and Description.

e) In the Operating System field, choose Chrome OS All.

f) In the Certificate Template field, select the required certificate template.
g) Click Submit. Observe that the SSID is provisioned via the Google Admin Console and not through the native supplicant provisioning flow.

**Step 2** Map the NSP in the Client Provisioning page.

a) Choose Policy > Client Provisioning.
b) Define the result.
   - Choose the in-built Native Supplicant configuration (Cisco-ISE-Chrome-NSP) in the Results of the client provisioning policy.
   - Or, create a new rule and ensure to choose the Result created for the Chromebook device.

---

**Wipe a Chromebook Device**

The Chromebook device must be wiped after the Google Admin Console is configured by the Google Administrator. The Chromebook user must wipe the device, which is a one-time process, to force extensions and configure the network settings. You can refer to the following URL: [https://support.google.com/chrome/a/answer/1360642](https://support.google.com/chrome/a/answer/1360642) for further information.

The Chromebook user performs the following steps:

**Step 1** Press Esc-Refresh-Power key combination. The screen displays a yellow exclamation point (!).

**Step 2** Press Ctrl-D key combination to begin dev mode, then press Enter key. The screen displays a red exclamation point.

**Step 3** Press Ctrl-D key combination. The Chromebook deletes its local data, returning to its initial state. The deletion takes approximately 15 minutes.

**Step 4** When the transition completes, press the Spacebar key, then press the Enter key to return to verified mode.

**Step 5** Enroll the Chromebook before signing in.

---

**What to do next**

Enroll Chromebook to the Google Admin Console.

---

**Enroll Chromebook to the Google Admin Console**

In order to provision a Chromebook device, the Chromebook user must first enroll in the Google Admin Console page and receive device policies and forced extensions.

**Step 1** Turn on the Chromebook device and follow the onscreen instructions until you see the sign on screen. Do not sign in yet.

**Step 2** Before signing in to the Chromebook device, press Ctrl-Alt-E key combination. The Enterprise Enrolment screen appears.

**Step 3** Enter your email address and click Next.
You will receive the following message: Your device has successfully been enrolled for enterprise management.

**Step 4** Click Done.
Step 5 Enter the username and password from your Google admin welcome letter, or the username and password for an existing Google Apps user on your account that has eligibility to enroll.

Step 6 Click Enroll Device. You will receive a confirmation message that the device has been successfully enrolled.

Note that the Chromebook enrollment is a one-time process.

**Connect Chromebook to the Cisco ISE Network for BYOD Onboarding**

The procedure is for Dual SSID—Open network to Dot1x network using EAP-TLS protocol. The Chromebook user performs the following steps:

- **Note** If you are using Dual SSID—Dot1x PEAP to an EAP-TLS network, you should connect to the network by entering your credentials in the network supplicant (not the web browser).

Step 1 In the Chromebook device, click Settings.

Step 2 In the Internet Connection section, click Provisioning Wi-Fi Network, and then click your network.

Step 3 You will be redirected to a credentialed guest portal.

1. In the Sign On page, enter the Username and Password.
2. Click Sign-on.

Step 4 In the BYOD Welcome page, click Start.

Step 5 In the Device Information field, enter a name for your device and a description. For example, Personal Devices: Jane's Chromebook Used for School or Shared Devices: Library Chromebook #1 or Classroom 1 Chromebook #1.

Step 6 Click Continue.

Step 7 Click Yes in the Cisco Network Setup Assistant dialog box to install the certificate to access the secure network.

If secure WiFi is configured by the Google Administrator, you should be connected automatically. However, if you are not connected, select the secure SSID from the available networks.

Chromebook device users who have already enrolled to the domain and have the Cisco Network Setup Assistant extension, can update the extension without waiting for the auto update. You can update the extension by following the steps below.

1. In your Chromebook device, open the browser and enter the following URL: chrome://Extensions.
2. Check the Developer Mode check box.
3. Click Update Extensions Now.
4. Verify that the Cisco Network Setup Assistant extension version is 2.1.0.35 and higher.
Google Admin Console - Wi-Fi Network Settings

The Wi-Fi network configuration is used to configure an SSID in a customer network or to match the certificate using certificate attributes (for EAP-TLS). When the certificate is installed in the Chromebook, it is synchronized with the Google admin settings. Connection is established only when one of the defined certificate attributes matches the SSID configuration.

Listed below are the mandatory fields, specific to EAP-TLS, PEAP, and Open network flows, which the Google administrator configures to set up the Wi-Fi network in the Google Admin Console page (Device Management > Network > Wi-Fi > Add Wi-Fi) for each Chromebook user.

<table>
<thead>
<tr>
<th>Field</th>
<th>EAP-TLS</th>
<th>PEAP</th>
<th>Open</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the network connection.</td>
<td>Enter the name of the network connection.</td>
<td>Enter the name of the network connection.</td>
</tr>
<tr>
<td>Service Set Identifier (SSID)</td>
<td>Enter the SSID (for example, tls ssid).</td>
<td>Enter the SSID (for example, tls ssid).</td>
<td>Enter the SSID (for example, tls ssid).</td>
</tr>
<tr>
<td>This SSID Is Not Broadcast</td>
<td>Select the option.</td>
<td>Select the option.</td>
<td>Select the option.</td>
</tr>
<tr>
<td>Automatically Connect</td>
<td>Select the option.</td>
<td>Select the option.</td>
<td>Select the option.</td>
</tr>
<tr>
<td>Security Type</td>
<td>WPA/WPA2 Enterprise (802.1x)</td>
<td>WPA/WPA2 Enterprise (802.1x)</td>
<td>Open</td>
</tr>
<tr>
<td>Extensible Authentication Protocol</td>
<td>EAP-TLS</td>
<td>PEAP</td>
<td>—</td>
</tr>
<tr>
<td>Inner Protocol</td>
<td>—</td>
<td>• Automatic</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MSCHAP v2 (Select the option)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MD5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PAP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MSCHAP</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• GTC</td>
<td></td>
</tr>
<tr>
<td>Outer Identity</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Username</td>
<td>Optional, either set a fixed value or use variables from the user login: ${LOGIN_ID} or ${LOGIN_EMAIL}.</td>
<td>Enter the PEAP credentials to authenticate against ISE (internal ISE user/AD/other ISE identities) and the Password field.</td>
<td>—</td>
</tr>
<tr>
<td>Field</td>
<td>EAP-TLS</td>
<td>PEAP</td>
<td>Open</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Server Certificate Authority</td>
<td>Select the ISE certificate (imported from Device Management &gt; Network &gt; Certificates).</td>
<td>Select the ISE certificate (imported from Device Management &gt; Network &gt; Certificates).</td>
<td>—</td>
</tr>
</tbody>
</table>
| Restrict Access to this Wi-Fi Network by Platform | • Select Mobile Devices.  
• Select Chromebooks.                                               | • Select Mobile Devices.  
• Select Chromebooks.                                                 | —     |
| Client Enrollment URL                   | Enter a URL to which the Chromebook device browser is redirected for users who are not enrolled. Configure ACLs on the Wireless LAN Controller for redirecting unenrolled users. | —                                                                | —     |
An attribute in the certificate. Select at least one attribute from either the Issuer Pattern or Subject Pattern that should match installed certificate attributes. Specify certificate attributes that will be matched with the Chromebook device to accept the certificate.

- **Common Name**: Refers to the Subject field of the certificate or the wildcard domain in the Subject field of the certificate, which must match the FQDN of the node.
- **Locality**: Refers to the test locality (City) that is associated with the certificate subject.
- **Organization**: Refers to the organization name that is associated with the certificate subject.
- **Organizational Unit**: Refers to the organizational unit name that is associated with the certificate subject.
<table>
<thead>
<tr>
<th>Field</th>
<th>EAP-TLS</th>
<th>PEAP</th>
<th>Open</th>
</tr>
</thead>
</table>
| Subject Pattern  | An attribute in the certificate. Select at least one attribute from either the Issuer Pattern or Subject Pattern that should match installed certificate attributes. Specify certificate attributes that will be matched with the Chromebook device to accept the certificate.  
  - Common Name: Refers to the Subject field of the certificate or the wildcard domain in the Subject field of the certificate, which must match the FQDN of the node.  
  - Locality: Refers to the test locality (City) that is associated with the certificate subject.  
  - Organization: Refers to the organization name that is associated with the certificate subject.  
  - Organizational Unit: Refers to the organizational unit name that is associated with the certificate subject. |      |      |
| Proxy Settings   | • Direct Internet Connection (Selected)  
  • Manual Proxy Configuration  
  • Automatic Proxy Configuration | • Direct Internet Connection (Selected)  
  • Manual Proxy Configuration  
  • Automatic Proxy Configuration |      |
Monitor Chromebook Device Activities in Cisco ISE

Cisco ISE provides various reports and logs to view information related to the authentication and authorization of Chromebook devices. You can run these reports either on demand or on regular basis. You can view the authentication method (for example, 802.1x) and authentication protocol (for example, EAP-TLS) in the Operations > RADIUS > Live Logs page. You can also identify the number of end points that are classified as Chromebook devices by navigating to the Work Centers > Network Access > Identities > Endpoints page.

Troubleshoot Chromebook Device Onboarding

This section describes problems that you may encounter while onboarding your Chromebook device.

- Error: Unable to install the extension from the webstore—You cannot install the extension from the webstore. It will be automatically installed on your Chromebook device by the network administrator.

- Error: Completed the installation of the certificate, however, unable to connect to the secure network—Verify on the Admin Console that the installed certificate matches defined Issuer/Subject attribute pattern. You can get information about installed certificate from: chrome://settings/certificates

- Error: Displays an error message "Obtain Network Certificate", when trying to manually connect to the secure network on the Chromebook—Click Get New Certificate, the browser opens and redirects you to the ISE BYOD flow to install the certificate. However, if you are unable to connect to the secure network, verify on the Admin Console that the installed certificate matches the defined Issuer/Subject attribute pattern.

- Error: Clicked Get New Certificate but is forwarded to the www.cisco.com site—User needs to be connected to the provisioning SSID, in order to be redirected to ISE and commence the certificate installation process. Be sure that the correct access list is defined for this network.

- Error: Displays an error message "Only managed devices can use this extension. Contact helpdesk or network administrator"—Chromebook is a managed device and the extension must be configured as a forced install to gain access to the Chrome OS APIs to install the certificate on the device. Although, the extension can be installed manually by downloading it from the Google web store, an unenrolled Chromebook user cannot install the certificate.

An unenrolled Chromebook device can secure a certificate if the user belongs to the Domain Users group. The extension tracks the domain user on any device. However, the domain user can produce user-based authentication keys for an unenrolled device.

- Error: Unclear of the order in which SSIDs are connected in the Google Admin Console—
  - If several SSIDs (PEAP and EAP-TLS) are configured on the Google Admin Console, after the certificate is installed and the attributes are matched, the Chrome OS automatically connects to the SSID with certificate-based authentication regardless of the order in which the SSIDs are configured.
  - If two EAP-TLS SSIDs match the same attribute, the connection depends on other factors such as signal strength and other network level signals, which cannot be controlled by the user or admin.

<table>
<thead>
<tr>
<th>Field</th>
<th>EAP-TLS</th>
<th>PEAP</th>
<th>Open</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply Network</td>
<td>By User</td>
<td>By User</td>
<td>—</td>
</tr>
</tbody>
</table>
• If multiple EAP-TLS certificates are installed on the Chromebook device and all of them match the certificate pattern configured on the Admin Console, the newest certificate will be used for the connection.

Create AnyConnect Configuration

AnyConnect configuration includes AnyConnect software and its associated configuration files. This configuration can be used in the client provisioning policy that allows users to download and install AnyConnect resources on the clients. If you use both ISE and an ASA to deploy AnyConnect, then the configurations must match on both headends.

Note
To push the ISE posture module when connected to a VPN, Cisco recommends that you install the AnyConnect agent through Cisco Adaptive Security Appliance (ASA), which uses the Cisco's Adaptive Security Device Manager (ASDM) GUI tool. ASA does the installation using the VPN downloader. With the download, the ISE posture profile is pushed via ASA, and the discovery host needed for later provisioning the profile is available before the ISE posture module contacts ISE. Whereas with ISE, the ISE posture module will get the profile only after ISE is discovered, which could result in errors. Therefore, ASA is recommended to push the ISE posture module when connected to a VPN.

Before you begin
You must upload the AnyConnect package, compliance module, profiles, and optionally any customization and localization bundles before configuring an AnyConnect Configuration object.

Step 1
Choose Policy > Policy Elements > Results > Client Provision > Resources.

Step 2
Click Add to create an AnyConnect configuration.

Step 3
Choose AnyConnect Configuration.

Step 4
Choose an AnyConnect Package, which you previously uploaded. For example, AnyConnectDesktopWindows xxx.x.xxxxx.x.

Step 5
Enter the name for the current AnyConnect Configuration. For example, AC Config xxx.x.xxxxx.x.

Step 6
Choose the compliance module, which you previously uploaded. For example, AnyConnectComplianceModulewindows x.x.xxxx.x

Step 7
Check one or more AnyConnect modules check boxes. For example, choose one or more modules from the following: ISE Posture, VPN, Network Access Manager, Web Security, AMP Enabler, ASA Posture, Start Before Log on (only for Windows OS), and Diagnostic and Reporting Tool.

Note
Un-checking the VPN module under AnyConnect Module Selection does not disable the VPN tile in the provisioned client. You must configure VPNDisable_ServiceProfile.xml to disable the VPN tile on AnyConnect GUI. In a system where AnyConnect is installed at the default location, you can find this file under C:\Program Files\Cisco. If AnyConnect is installed at a different location, then the file will be available under <AnyConnect Installed path>\Cisco.

Step 8
Choose AnyConnect profiles for selected AnyConnect modules. For example, ISE Posture, VPN, NAM, and Web Security.

Step 9
Choose AnyConnect customization and localization bundles.
Create a Posture Agent Profile

Use this procedure to create an AnyConnect posture agent profile, where you can specify parameters that define the agent behavior for the posture protocol.

Step 1 Choose Policy > Policy Elements > Results > Client Provisioning > Resources.

Step 2 Click Add.

Step 3 Choose NAC AnyConnect Agent Posture Profile.

Step 4 Under Posture Agent Profile Settings, choose AnyConnect.

Step 5 Configure parameters for the following:
   • Cisco ISE posture agent behavior
   • Client IP Address Changes
   • Cisco ISE posture protocol

Step 6 Click Submit.

Client IP Address Refresh Configuration

The following table describes the fields in the NAC AnyConnect Posture Profile page, which allows you to configure parameters for the client to renew or refresh its IP address after VLAN change. The navigation path for this page is Policy > Policy Elements > Results > Client Provisioning > Resources > Add > NAC or AnyConnect Posture Profile.
<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>Mode (Applies only to Cisco NAC Agent)</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN detection interval</td>
<td>0, 5</td>
<td>Merge</td>
<td>This setting is the interval at which the agent check for the VLAN change.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For the Windows NAC agent, the default value is 0. By default, the access to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>authentication VLAN change feature is disabled for Windows. The valid range is 0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>to 5 seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For the Mac OS X agent, the default value is 5. By default, the access to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>authentication VLAN change feature is enabled with VlanDetectInterval as 5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>seconds for Mac OS X. The valid range is 5 to 900 seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 — Access to Authentication VLAN change feature is disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 to 5 — Agent sends an Internet Control Message Protocol (ICMP) or Address</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Resolution Protocol (ARP) query every 5 seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6 to 900 — An ICMP or ARP query is sent every x seconds.</td>
</tr>
<tr>
<td>Enable VLAN detection without UI (Not applicable for a Mac OS X client)</td>
<td>No</td>
<td>Merge</td>
<td>This setting enables or disables VLAN detection even when the user is not</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>logged in.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>No — VLAN detect feature is disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Yes — VLAN detect feature is enabled.</td>
</tr>
<tr>
<td>Field</td>
<td>Default Value</td>
<td>Mode (Applies only to Cisco NAC Agent)</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------------</td>
<td>----------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Retry detection count</td>
<td>3</td>
<td>Merge</td>
<td>If the Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP) polling fails, this setting configures the agent to retry x times before refreshing the client IP address.</td>
</tr>
</tbody>
</table>
| Ping or ARP                   | 0 (The valid range is 0 to 2.) | Merge                                  | This setting specifies the method used for detecting the client IP address change.  
0—Poll using ICMP  
1—Poll using ARP  
2—Poll using ICMP first, then (if ICMP fails) ARP |
| Maximum timeout for ping      | 1 (The valid range is 1 to 10 seconds.) | Merge                                  | Poll using ICMP, and if there is no response within the specified time, then declare an ICMP polling failure. |
| Enable agent IP refresh       | Yes (Default) | Overwrite                              | This setting specifies whether or not the client machine to renew or refresh its IP address after the switch (or WLC) changes the VLAN for the login session of the client on the respective switch port. |
| DHCP renew delay              | 0 (The valid range is 0 to 60 seconds.) | Overwrite                              | This setting specifies that the client machine waits before attempting to request for a new IP address from the network DHCP server. |
| DHCP release delay            | 0 (The valid range is 0 to 60 seconds.) | Overwrite                              | The setting specifies that the client machine waits before releasing its current IP address. |
Merge parameter values with existing agent profile settings or overwrite them to appropriately configure clients on Windows and Mac OS X clients for refreshing IP addresses.

Posture Protocol Settings

The following table describes the fields in the NAC or AnyConnect Posture Profile page, which allows you to configure posture protocol settings for AnyConnect in Cisco ISE. For information on other fields in posture protocol settings for AnyConnect, see the Cisco AnyConnect Secure Mobility Client Administrator Guide for your version of AnyConnect.

<table>
<thead>
<tr>
<th>Field</th>
<th>Default Value</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call Home List</td>
<td>—</td>
<td>Enter a comma-separated list of IP addresses and ports with colon in between the IP address and the port.</td>
</tr>
<tr>
<td>Back-off Timer</td>
<td>30 sec</td>
<td>This setting enables the AnyConnect agent to continuously to reach the discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached. The valid range is 10 to 600 seconds.</td>
</tr>
</tbody>
</table>

Client Login Session Criteria

Cisco ISE looks at various elements when classifying the type of login session through which users access the internal network, including:

- Client machine operating system and version
- Client machine browser type and version
- Group to which the user belongs
- Condition evaluation results (based on applied dictionary attributes)

After Cisco ISE classifies a client machine, it uses client provisioning resource policies to ensure that the client machine is set up with an appropriate agent version, up-to-date compliance modules for antivirus and antispyware vendor support, and correct agent customization packages and profiles, if necessary.
Agent Download Issues on Client Machine

Problem
The client machine browser displays a “no policy matched” error message after user authentication and authorization. This issue applies to user sessions during the client provisioning phase of authentication.

Possible Causes
The client provisioning policy is missing required settings.

Posture Agent Download Issues
Remember that downloading the posture agent installer requires the following:

- The user must allow the ActiveX installer in the browser session the first time an agent is installed on the client machine. (The client provisioning download page prompts for this.)
- The client machine must have Internet access.

Resolution
- Ensure that a client provisioning policy exists in Cisco ISE. If yes, verify the policy identity group, conditions, and type of agent(s) defined in the policy. (Also ensure whether or not there is any agent profile configured under Policy > Policy Elements > Results > Client Provisioning > Resources > Add > NAC or AnyConnect Posture Profile, even a profile with all default values.)
- Try re-authenticating the client machine by bouncing the port on the access switch.

Cisco ISE Posture Agents
Posture agents are applications that reside on client machines logging into the Cisco ISE network. Agents can be persistent (like the AnyConnect for Windows and Mac OS X) and remain on the client machine after installation, even when the client is not logged into the network. Agents can also be temporal (like the Cisco Temporal Agent for Windows and Mac OS), removing themselves from the client machine after the login session has terminated. In either case, the Agent helps the user to log in to the network, receive the appropriate access profile, and even perform posture assessment on the client machine to ensure it complies with network security guidelines before accessing the core of the network.

Note
The Cisco Temporal Agent for Windows supports the Client Provisioning Portal and uses URL redirection.

Posture Agent Discovery Request and Cisco ISE Response
Cisco ISE supports coexistence of AnyConnect and legacy Cisco ISE NAC agents on Windows and Mac OS x clients. Agents start the posture discovery probe only when there is any change in the network on the clients. Cisco ISE responds to the client's posture discovery probe based on the client provisioning policy and the corresponding agent will get the discovery response, which results in only one agent being active.
Based on the client provisioning policy, Cisco ISE differs in responding to the agents posture discovery probe as below:

- If the endpoint is configured to use the legacy agent (Cisco ISE NAC agent for Windows and MacOSx), the agent receives the discovery response with a string "X-perfigo-CAS=FQDN" in the existing format. AnyConnect stops discovery, if the discovery response is received for the legacy agent.

- If the endpoint is configured to use AnyConnect, Cisco ISE responds in a different format. This will be the Cisco ISE Policy Service node FQDN and the AnyConnect Configuration URL, AnyConnect package location and version based on the client provisioning policy. The legacy agent stops discovery, if the response is received for AnyConnect.

Note

MAC OSX devices do not send requests to default gateway. These devices use only the following two probes:

- discovery host
- enroll.cisco.com

Ensure that you have configured correct DNS on MAC OSX devices to resolve enroll.cisco.com.

Web Agent Posture Discovery Request and Cisco ISE Response

The Web agent does not do discovery probe. If an endpoint is configured to use the Web agent, Cisco ISE responds using the format, X-ISE-PDP-WEBAAGENT=FQDN". The webagent discovery response is used to invoke the Cisco NAC Agent on the client, if the client provisioning policy is configured to use the Web agent.

Agent Displays “Temporary Access”

Problem

A client machine is granted “Temporary Access” to the network following login and authentication, but administrator and users expect full network access.

Possible Causes

This issue is applicable to any client machine login session using an agent to connect.

If the Cisco NAC Agent is running on the client and:

- The interface on the client machine goes down
- The session is terminated

Resolution

The user must try to verify network connectivity and then try to log in again (and pass through posture assessment, as well) to attempt to reestablish the connection.
Agent Fails to Initiate Posture Assessment

Problem
The user is presented with a “Clean access server not available” message. This issue applies to any agent authentication session from Cisco ISE.

Possible Cause
This error could mean that either the session has terminated or Cisco ISE is no longer reachable on the network.

Resolution
• The user can try to log into the network again.
• The user can try to ping the default gateway or the RADIUS server IP address or FQDN supplied by the network administrator.
• The administrator can check network access attributes for the user (like the assigned VLAN, ACLs, routing, execute the `nslookup` command on the client, client machine DNS connection, and so on).

AnyConnect
Cisco ISE uses an integrated module in AnyConnect for Cisco ISE posture requirements. AnyConnect is the posture agent that coexists with Cisco ISE NAC Agent on the same endpoint. Based on the client provisioning policy configuration in Cisco ISE, only one of the agents will be active at a time.

Note
Cisco AnyConnect is not supported in CWA flow. It cannot be provisioned from the Guest portal using the `Require guest device compliance` field in the `Work Centers > Guest Access > Portals & Components > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Guest Device Compliance Settings` page. Instead, AnyConnect should be provisioned from the Client Provisioning portal as a result of redirection configured in authorization permissions.

Note
When switching network mediums, the AnyConnect ISE posture module requires a change of the default gateway to detect a network change and reassess the client.

To leverage Cisco ISE for integration with AnyConnect agent, Cisco ISE:
• Serves as a staging server to deploy AnyConnect, Version 4.0 and its future releases
• Interacts with AnyConnect posture component for Cisco ISE posture requirements
• Supports deployment of AnyConnect profiles, customization/language packages, and OPSWAT library updates for Windows and Mac OS x operating systems
• Supports AnyConnect and legacy agents at the same time
Cisco Web Agent

The Cisco Web Agent provides temporal posture assessment for client machines.

Users can launch the Cisco Web Agent executable, which installs the Web Agent files in a temporary directory on the client machine via ActiveX control or Java applet.

After users log in to the Cisco Web Agent, the Web Agent gets the requirements that are configured for the user role and the operating system from the Cisco ISE server, checks the host registry, processes, applications, and services for required packages and sends a report back to the Cisco ISE server. If requirements are met on the client machine, the user is allowed network access. If requirements are not met, the Web Agent presents a dialog to the user for each requirement that is not satisfied. The dialog provides the user with instructions and the action to take for the client machine to meet the requirement. Alternatively, if the specified requirements are not met, users can choose to accept the restricted network access while they try to remediate the client system so that it meets requirements for the user login role.

---

**Note**

ActiveX is supported only on the 32-bit versions of Internet Explorer. You cannot install ActiveX on a Firefox web browser or on a 64-bit version of Internet Explorer.

Configure Client Provisioning Resource Policies

For clients, the client provisioning resource policies determine which users receive which version (or versions) of resources (agents, agent compliance modules, and/or agent customization packages/profiles) from Cisco ISE upon login and user session initiation.

For AnyConnect, resources can be selected either from the client provisioning resources page to create an AnyConnect configuration that you can use in the client provisioning policy page. AnyConnect configuration is the AnyConnect software and its association with different configuration files that includes AnyConnect binary package for Windows and Mac OS X clients, compliance module. module profiles, customization and language packages for AnyConnect.

**Before you begin**

- Before you can create effective client-provisioning resource policies, ensure that you have added resources to Cisco ISE. When you download the agent compliance module, it always overwrites the existing one, if any, available in the system.

- Check the native supplicant profile that is used in the client provisioning policy and ensure that the wireless SSID is correct. For iOS devices, if the network that you are trying to connect to is hidden, check the **Enable if target network is hidden** check box from the iOS Settings area.

- Refer to the **Prerequisite for Certificate-Based Conditions** section for client provisioning rules that include conditions based on certificate attributes.

**Step 1**  Choose Policy > Client Provisioning.

**Step 2**  Choose Enable, Disable, or Monitor from the behavior drop-down list:
• **Enable**—Ensures Cisco ISE uses this policy to help fulfill client-provisioning functions when users log in to the network and conform to the client-provisioning policy guidelines.

• **Disable**—Cisco ISE does not use the specified resource policy to fulfill client-provisioning functions.

• **Monitor**—Disables the policy and “watches” the client-provisioning session requests to see how many times Cisco ISE tries to invoke based on the “Monitored” policy.

**Step 3** Enter a name for the new resource policy in the Rule Name text box.

**Step 4** Specify one or more Identity Groups to which a user who logs into Cisco ISE might belong.

You can choose to specify the Any identity group type, or choose one or more groups from a list of existing Identity Groups that you have configured.

**Step 5** Use the Operating Systems field to specify one or more operating systems that might be running on the client machine or device through which the user is logging into Cisco ISE.

You can choose to specify a single operating system like "Android", "Mac OS", and "Mac OS X" or an umbrella operating system designation that addresses a number of client machine operating systems like "Windows XP (All)" or "Windows 7 (All)."

**Note** Though the option to select MAC OS 10.6/10.7/10.8 is available in the client provisioning policy page in Cisco ISE GUI, these versions are not supported by AnyConnect.

**Step 6** In the Other Conditions field, specify a new expression that you want to create for this particular resource policy.

**Step 7** For client machines, use **Agent Configuration** to specify which agent type, compliance module, agent customization package, and/or profile to make available and provision on the client machine.

It is mandatory to include the client provisioning URL in authorization policy, to enable the NAC Agent to popup in the client machines. This prevents request from any random clients and ensures that only clients with proper redirect URL can request for posture assessment.

**Step 8** Click **Save**.

---

**What to do next**

Once you have successfully configured one or more client provisioning resource policies, you can start to configure Cisco ISE to perform posture assessment on client machines during login.

**Configure Cisco ISE Posture Agent in the Client Provisioning Policy**

For client machines, configure which agent type, compliance module, agent customization package, and/or profile to make available and provision for users to download and install on the client machine.

**Before you begin**

You must have added client provisioning resources for AnyConnect and Cisco ISE NAC in Cisco ISE.

**Step 1** Choose an available agent from the **Agent** drop-down list and specify whether the agent upgrade (download) defined here is mandatory for the client machine by enabling or disabling the **Is Upgrade Mandatory** option, as appropriate.
The **Is Upgrade Mandatory** setting only applies to agent downloads. Agent profile, compliance module, and Agent customization package updates are always mandatory.

**Step 2** Choose an existing agent profile from the **Profile** drop-down list.

**Step 3** Choose an available compliance module to download to the client machine using the **Compliance Module** drop-down list.

**Step 4** Choose an available agent customization package for the client machine from the **Agent Customization Package** drop-down list.

---

**Configure Native Supplicants for Personal Devices**

Employees can connect their personal devices to the network directly using native supplicants, which are available for Windows, Mac OS, iOS, and Android devices. For personal devices, specify which Native Supplicant configuration to make available and provision on the registered personal device.

**Before you begin**

Create native supplicant profiles so that when user log in, based on the profile that you associate with that users authorization requirements , Cisco ISE provides the necessary supplicant provisioning wizard to set up the users personal devices to access the network.

**Step 1** Choose **Policy > Client Provisioning**.

**Step 2** Choose **Enable**, **Disable**, or **Monitor** from the behavior drop-down list:

**Step 3** Enter a name for the new resource policy in the Rule Name text box.

**Step 4** Specify the following:

- Use the Identity Groups field to specify one or more Identity Groups to which a user who logs into Cisco ISE might belong.
- Use the Operating System field to specify one or more operating systems that might be running on the personal device through which the user is logging into Cisco ISE.
- Use the Other Conditions field to specify a new expression that you want to create for this particular resource policy.

**Step 5** For personal devices, use **Native Supplicant Configuration** to choose the specific **Configuration Wizard** to distribute to these personal devices.

**Step 6** Specify the applicable **Wizard Profile** for the given personal device type.

**Step 7** Click **Save**.

---

**Client Provisioning Reports**

You can access the Cisco ISE monitoring and troubleshooting functions to check on overall trends for successful or unsuccessful user login sessions, gather statistics about the number and types of client machines logging into the network during a specified time period, or check on any recent configuration changes in client provisioning resources.
Client Provisioning Requests

The Operations > Reports > ISE Reports > Endpoints and Users > Client Provisioning report displays statistics about successful and unsuccessful client provisioning requests. When you choose Run and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting client provisioning data.

Supplicant Provisioning Requests

The Operations > Reports > ISE Reports > Endpoints and Users > Supplicant Provisioning window displays information about recent successful and unsuccessful user device registration and supplicant provisioning requests. When you choose Run and specify one of the preset time periods, Cisco ISE combs the database and displays the resulting supplicant provisioning data.

The Supplicant Provisioning report provides information about a list of endpoints that are registered through the device registration portal for a specific period of time, including data like the Logged at Date and Time, Identity (user ID), IP Address, MAC Address (endpoint ID), Server, profile, Endpoint Operating System, SPW Version, Failure Reason (if any), and the Status of the registration.

Client Provisioning Event Logs

You can search event log entries to help diagnose a possible problem with client login behavior. For example, you may need to determine the source of an issue where client machines on your network are not able to get client provisioning resource updates upon login. You can use logging entries for Posture and Client Provisioning Audit and Posture and Client Provisioning Diagnostics.
CHAPTER 26

Configure Client Posture Policies

Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the state, also known as posture, of all the endpoints that are connecting to a network for compliance with corporate security policies. This allows you to control clients to access protected areas of a network.

- Posture Service, on page 772
- Posture Administration Settings, on page 775
- Download Posture Updates to Cisco ISE, on page 779
- Configure Acceptable Use Policies for Posture Assessment, on page 780
- Posture Conditions, on page 780
- Simple Posture Conditions, on page 781
- Create Simple Posture Conditions, on page 781
- Compound Posture Conditions, on page 782
- Predefined Condition for Enabling Automatic Updates in Windows Clients, on page 782
- Preconfigured Antivirus and Antispyware Conditions, on page 782
- Antivirus and Antispyware Support Chart, on page 783
- Compliance Module, on page 783
- Create Compound Posture Conditions, on page 784
- Create Patch Management Conditions, on page 785
- Create Disk Encryption Conditions, on page 785
- Configure Posture Policies, on page 786
- Prerequisite for Certificate-Based Conditions, on page 787
- Default Posture Policies, on page 788
- Posture Assessment Options, on page 789
- Posture Remediation Options, on page 790
- Custom Conditions for Posture, on page 791
- Posture End-Point Custom Attributes, on page 791
- Create Posture Policy Using End-Point Custom Attributes, on page 791
- Custom Posture Remediation Actions, on page 792
- Posture Assessment Requirements, on page 796
- Custom Permissions for Posture, on page 798
- Configure Standard Authorization Policies, on page 799
- Best Practices for Network Drive Mapping with Posture, on page 799
- AnyConnect Stealth Mode Workflow, on page 799
- Posture Types, on page 803
Posture Service

Posture is a service in Cisco Identity Services Engine (Cisco ISE) that allows you to check the compliance, also known as posture, of endpoints, before allowing them to connect to your network. A posture agent, such as the AnyConnect ISE Posture Agent, runs on the endpoint. Client Provisioning ensures that the endpoints receive the appropriate Posture Agent.

The ISE Posture Agent for Cisco ISE does not support Windows Fast User Switching when using the native supplicant, because there is no clear disconnect of the previous user. When a new user is sent, the Agent is hung on the old user process and session ID, so a new posture session cannot start. As per the Microsoft Security policies, it is recommended to disable Fast User Switching.

Note

In ISE, session control is done on multiple nodes.

On an MnT node, sessions are removed:

• If there was accounting start, but no accounting stop (stale session), the session is removed in five days.
• If there was accounting start followed by accounting stop, the session is removed in a few hours.
• If there was no accounting start or stop, the session is removed in a few hours.

On a PSN node, sessions are removed:

• When accounting stop is received.
• When the session cache is cleared, especially when there are many sessions, or you reload the PSN.

If posture without redirection is used in multinode deployment, and sessions are not properly managed, it may impact the posture functionality.

ISE Community Resource

Configure ISE 2.1 and AnyConnect 4.3 Posture USB Check
How To Configure Posture with AnyConnect Compliance Module and ISE 2.0

Related Topics

Components of Posture Services, on page 772
Posture and Client-Provisioning Policies Workflow, on page 774
Posture Service Licenses, on page 774

Components of Posture Services

Cisco ISE posture service primarily includes the posture administration services and the posture run-time services.
Posture Administration Services

If you have not installed the Apex license in Cisco ISE, then the posture administration services option is not available from the Admin portal.

Administration services provide the back-end support for posture-specific custom conditions and remediation actions that are associated with the requirements and authorization policies that are configured for posture service.

Posture Run-Time Services

The posture run-time services encapsulate all the interactions that happen between the client agent and the Cisco ISE server for posture assessment and remediation of clients.

Posture run-time services begin with the Discovery Phase. An endpoint session is created after the endpoint passes 802.1x authentication. The client agent then attempts to connect to a Cisco ISE node by sending discovery packets through different methods in the following order:

1. via HTTP to Port 80 on a Cisco ISE server (if configured)
2. via HTTPS to Port 8905 on a Cisco ISE server (if configured)
3. via HTTP to Port 80 on the default gateway
4. via HTTPS to Port 8905 to each previously contact server
5. via HTTP to Port 80 on enroll.cisco.com

The Posture Phase begins when the Acceptable User Policy (if any) is accepted. The Cisco ISE node issues a posture token for the Posture Domain to the client agent. The posture token allows the endpoint to reconnect to the network without going through the posture process again. It contains information such as the Agent GUID, the Acceptable User Policy status, and endpoint operating system information.

The messages used in the Posture Phase are in the NEA PB/PA format (RFC5792).
Posture and Client-Provisioning Policies Workflow

Cisco ISE provides you with three types of licenses, the Base license, the Plus license, and the Apex license. If you have not installed the Apex license on the Primary PAN, then the posture requests will not be served in Cisco ISE. The posture service of Cisco ISE can run on a single node or on multiple nodes.

Posture Service Deployment

You can deploy Cisco ISE in a standalone environment (on a single node) or in a distributed environment (on multiple nodes).

In a standalone Cisco ISE deployment, you can configure a single node for all the administration services, the monitoring and troubleshooting services, and the policy run-time services.

In a distributed Cisco ISE deployment, you can configure each node as a Cisco ISE node for administration services, monitoring and troubleshooting services, and policy run-time services. A node that runs the administration services is the primary node in that Cisco ISE deployment. The other nodes that run other services are the secondary nodes which can be configured for backup services for one another.
Enable Posture Session Service in Cisco ISE

Before you begin

- You must enable session services in Cisco ISE and install the advanced license package to serve all the posture requests received from the clients.
- If you have more than one node that is registered in a distributed deployment, all the nodes that you have registered appear in the Deployment Nodes page, apart from the primary node. You can configure each node as a Cisco ISE node (Administration, Policy Service, and Monitoring personas).
- The posture service only runs on Cisco ISE nodes that assume the Policy Service persona and does not run on Cisco ISE nodes that assume the administration and monitoring personas in a distributed deployment.

Step 1
Choose Administration > System > Deployment > Deployment.

Step 2
Choose a Cisco ISE node from the Deployment Nodes window.

Step 3
Click Edit.

Step 4
Under the General Settings tab, check the Policy Service check box,
If the Policy Service check box is unchecked, both the session services and the profiling service check boxes are disabled.

Step 5
Check the Enable Session Services check box, for the Policy Service persona to run the Network Access, Posture, Guest, and Client Provisioning session services. To stop the session services, uncheck the check box.

Step 6
Click Save.

Run the Posture Assessment Report

You can run the Posture Detail Assessment report to generate a detailed status of compliance of the clients against the posture policies that are used during posture assessment.

Step 1
Choose Operations > Reports > ISE Reports > Endpoints and Users > Posture Detail Assessment.

Step 2
From the Time Range drop-down list, choose the specific time period.

Step 3
Click Run to view the summary of all the end points that were active during the selected time period.

Posture Administration Settings

You can globally configure the Admin portal for posture services. You can download updates automatically to the Cisco ISE server through the web from Cisco. You can also update Cisco ISE manually offline later. In addition, having an agent like AnyConnect, the NAC Agent, or the Web Agent installed on the clients provides posture assessment and remediation services to clients. The client agent periodically updates the compliance status of clients to Cisco ISE. After login and successful requirement assessment for posture, the client agent displays a dialog with a link that requires end users to comply with terms and conditions of network...
usage. You can use this link to define network usage information for your enterprise network that end users accept before they can gain access to your network.

Related Topics
   Timer Settings for Clients, on page 776
   Set Posture Status for Nonagent Devices, on page 777
   Posture Lease, on page 778
   Configure Acceptable Use Policies for Posture Assessment, on page 780

Timer Settings for Clients

You can set up timers for users to remediate, to transition from one state to another, and to control the login success screen.

We recommend configuring agent profiles with remediation timers and network transition delay timers as well as the timer used to control the login success screen on client machines so that these settings are policy based. You can configure all these timers for agents in client provisioning resources in the NAC or AnyConnect Posture Profile window (Policy > Policy Elements > Results > Client Provisioning > Resources > Add > NAC or AnyConnect Posture Profile).

However, when there are no agent profiles configured to match the client provisioning policies, you can use the settings in the General Settings configuration window (Administration > System > Settings > Posture > General Settings).

Related Topics
   Set Remediation Timer for Clients to Remediate Within Specified Time, on page 776
   Set Network Transition Delay Timer for Clients to Transition, on page 776
   Set Login Success Window to Close Automatically, on page 777

Set Remediation Timer for Clients to Remediate Within Specified Time

You can configure the timer for client remediation within a specified time. When clients fail to satisfy configured posture policies during an initial assessment, the agent waits for the clients to remediate within the time configured in the remediation timer. If the client fails to remediate within this specified time, then the client agent sends a report to the posture run-time services after which the clients are moved to the noncompliance state.

Step 1  Choose Administration > System > Settings > Posture > General Settings.
Step 2  In the Remediation Timer field, enter a time value in minutes.
        The default value is 4 minutes. The valid range is 1 to 300 minutes.
Step 3  Click Save.

Set Network Transition Delay Timer for Clients to Transition

You can configure the timer for clients to transition from one state to the other state within a specified time using the network transition delay timer, which is required for Change of Authorization (CoA) to complete. It may require a longer delay time when clients need time to get a new VLAN IP address during success and failure of posture. When successfully postured, Cisco ISE allows clients to transition from unknown to
compliant mode within the time specified in the network transition delay timer. Upon failure of posture, Cisco ISE allows clients to transition from unknown to noncompliant mode within the time specified in the timer.

---

**Step 1** Choose Administration > System > Settings > Posture > General Settings.

**Step 2** Enter a time value in seconds, in the Network Transition Delay field.

The default value is 3 seconds. The valid range is 2 to 30 seconds.

**Step 3** Click Save.

---

**Set Login Success Window to Close Automatically**

After successful posture assessment, the client agent displays a temporary network access screen. The user needs to click the OK button in the login window to close it. You can set up a timer to close this login screen automatically after specified time.

---

**Step 1** Choose Administration > System > Settings > Posture > General Settings.

**Step 2** Check the Automatically Close Login Success Screen After check box.

**Step 3** Enter a time value in seconds, in the field next to Automatically Close Login Success Screen After check box.

The valid range is 0 to 300 seconds. If the time is set to zero, then AnyConnect does not display the login success screen.

**Step 4** Click Save.

---

**Set Posture Status for Nonagent Devices**

You can configure the posture status of endpoints that run on non-agent devices like Linux or iDevices. When Android devices and Apple iDevices such as an iPod, iPhone, or iPad connect to a Cisco ISE enabled network, these devices assume the Default Posture Status settings.

These settings can also be applied to endpoints that run on Windows and Macintosh operating systems when a matching policy is not found during posture runtime.

**Before you begin**

In order to enforce policy on an endpoint, you must configure a corresponding Client Provisioning policy (Agent installation package). Otherwise, the posture status of the endpoint automatically reflects the default setting.

---

**Step 1** Choose Administration > System > Settings > Posture > General Settings.

**Step 2** From the Default Posture Status drop-down list, choose the option as Compliant or Noncompliant.

**Step 3** Click Save.
Posture Lease

You can configure Cisco ISE to perform posture assessment every time a user logs into your network or perform posture assessment in specified intervals. The valid range is 1 to 365 days.

This configuration applies only for those who use AnyConnect agent for posture assessment.

Periodic Reassessments

Periodic reassessment (PRA) can be done only for clients that are already successfully postured for compliance. PRA cannot occur if clients are not compliant on your network.

A PRA is valid and applicable only if the endpoints are in a compliant state. The policy service node checks the relevant policies, and compiles the requirements depending on the client role that is defined in the configuration to enforce a PRA. If a PRA configuration match is found, the policy service node responds to the client agent with the PRA attributes that are defined in the PRA configuration for the client before issuing a CoA request. The client agent periodically sends the PRA requests based on the interval specified in the configuration. The client remains in the compliant state if the PRA succeeds, or the action configured in the PRA configuration is to continue. If the client fails to meet PRA, then the client is moved from the compliant state to the noncompliant state.

The PostureStatus attribute shows the current posture status as compliant in a PRA request instead of unknown even though it is a posture reassessment request. The PostureStatus is updated in the Monitoring reports as well.

When the posture lease has not expired, an endpoint becomes compliant based on the Access Control List (ACL), and PRA is initiated. If PRA fails, the endpoint is deemed noncompliant and the posture lease is reset.

Configure Periodic Reassessments

You can configure periodic reassessments only for clients that are already successfully postured for compliance. You can configure each PRA to a user identity group that is defined in the system.

Before you begin

- Ensure that each PRA configuration has a unique group or a unique combination of user identity groups assigned to the configuration.
- You can assign a role_test_1 and a role_test_2, which are the two unique roles to a PRA configuration. You can combine these two roles with a logical operator and assign the PRA configuration as a unique combination of two roles. For example, role_test_1 OR role_test_2.
- Ensure that two PRA configurations do not have a user identity group in common.
- If a PRA configuration already exists with a user identity group “Any”, you cannot create other PRA configurations unless you perform one of the following:
  - Update the existing PRA configuration with the Any user identity group to reflect a user identity group other than Any.
  - Delete the existing PRA configuration with a user identity group “Any”.

---

Step 1  Choose Administration > System > Settings > Posture > Reassessments.
**Download Posture Updates to Cisco ISE**

Posture updates include a set of predefined checks, rules, and support charts for antivirus and antispyware for both Windows and Macintosh operating systems, and operating systems information that are supported by Cisco. You can also update Cisco ISE offline from a file on your local system, which contains the latest archives of updates.

When you deploy Cisco ISE on your network for the first time, you can download posture updates from the web. This process usually takes approximately 20 minutes. After the initial download, you can configure Cisco ISE to verify and download incremental updates to occur automatically.

Cisco ISE creates default posture policies, requirements, and remediations only once during an initial posture updates. If you delete them, Cisco ISE does not create them again during subsequent manual or scheduled updates.

**Before you begin**

To ensure that you are able to access the appropriate remote location from which you can download posture resources to Cisco ISE, you may be required to verify that you have the correct proxy settings configured for your network as described in Specifying Proxy Settings in Cisco ISE, page 5-2.

You can use the Posture Update page to download updates dynamically from the web.

**Step 1** Choose **Administration > System > Settings > Posture > Updates**.

**Step 2** Choose the **Web** option to download updates dynamically.

**Step 3** Click **Set to Default** to set the Cisco default value for the **Update Feed URL** field.

If your network restricts URL-redirection functions (via a proxy server, for example) and you are experiencing difficulty accessing the above URL, try also pointing your Cisco ISE to the alternative URL in the related topics.

**Step 4** Modify the values in the **Posture Updates** page.

**Step 5** Click **Update Now** to download updates from Cisco.

**Step 6** Click **OK** to continue with other tasks on Cisco ISE.

After being updated, the Posture Updates page displays the current Cisco updates version information as a verification of an update under Update Information section in the Posture Updates page.

**Related Topics**

- **Download Posture Updates Automatically**, on page 780
Download Posture Updates Automatically

After an initial update, you can configure Cisco ISE to check for the updates and download them automatically.

Before you begin

- You should have initially downloaded the posture updates to configure Cisco ISE to check for the updates and download them automatically.

Step 1
Choose Administration > System > Settings > Posture > Updates.

Step 2
In the Posture Updates page, check the Automatically check for updates starting from initial delay check box.

Step 3
Enter the initial delay time in hh:mm:ss format.
Cisco ISE starts checking for updates after the initial delay time is over.

Step 4
Enter the time interval in hours.
Cisco ISE downloads the updates to your deployment at specified intervals from the initial delay time.

Step 5
Click Yes to continue.

Step 6
Click Save.

Configure Acceptable Use Policies for Posture Assessment

After login and successful posture assessment of clients, the client agent displays a temporary network access screen. This screen contains a link to an acceptable use policy (AUP). When users click the link, they are redirected to a page that displays the network-usage terms and conditions, which they must read and accept.

Each Acceptable Use Policy configuration must have a unique user identity group, or a unique combination of user identity groups. Cisco ISE finds the AUP for the first matched user identity group, and then it communicates to the client agent that displays the AUP.

Step 1
Choose Administration > System > Settings > Posture > Acceptable Use Policy.

Step 2
Click Add.

Step 3
Modify the values in the New Acceptable Use Policy Configuration page.

Step 4
Click Submit.

Posture Conditions

A posture condition can be any one of the following simple conditions: a file, a registry, an application, a service, or a dictionary condition. One or more conditions from these simple conditions form a compound condition, which can be associated to a posture requirement.
When you deploy Cisco ISE on your network for the first time, you can download posture updates from the web for the first time. This process is called the initial posture update.

After an initial posture update, Cisco ISE also creates Cisco defined simple and compound conditions. Cisco defined simple conditions have pc_ as their prefixes and compound conditions have pr_ as their prefixes.

You can also configure Cisco ISE to download the Cisco-defined conditions periodically as a result of dynamic posture updates through the web. You cannot delete or edit Cisco defined posture conditions.

A user defined condition or a Cisco defined condition includes both simple conditions and compound conditions.

**Simple Posture Conditions**

You can use the Posture Navigation pane to manage the following simple conditions:

- **File Conditions**—A condition that checks the existence of a file, the date of a file, and the versions of a file on the client.

- **Registry Conditions**—A condition that checks for the existence of a registry key or the value of the registry key on the client.

- **Application Conditions**—A condition that checks if an application or process is running or not running on the client.

  ![Note](image)

  If a process is installed and running, user is compliant. However, the Application condition works in reverse logic; If an application is not installed and not running, the end user is complaint. If an application is installed and running, the end user is non-compliant.

- **Service Conditions**—A condition that checks if a service is running or not running on the client.

- **Dictionary Conditions**—A condition that checks a dictionary attribute with a value.

- **USB Conditions**—A condition that checks for the presence of USB mass storage device.

**Related Topics**

- [File Condition Settings](#), on page 1092
- [Registry Condition Settings](#), on page 1097
- [Application Condition Settings](#), on page 1099
- [Service Condition Settings](#), on page 1101
- [Dictionary Simple Condition Settings](#), on page 1108
- [USB Condition Settings](#), on page 1114

**Create Simple Posture Conditions**

You can create file, registry, application, service, and dictionary simple conditions that can be used in posture policies or in other compound conditions.
Before you begin

To perform the following task, you must be a Super Admin or Policy Admin.

---

<table>
<thead>
<tr>
<th>Step</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Choose <strong>Policy</strong> &gt; <strong>Policy Elements</strong> &gt; <strong>Conditions</strong> &gt; <strong>Posture</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>Choose any one of the following: <strong>File</strong>, <strong>Registry</strong>, <strong>Application</strong>, <strong>Service</strong>, or <strong>Dictionary Simple Condition</strong>.</td>
</tr>
<tr>
<td>3</td>
<td>Click <strong>Add</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>Enter the appropriate values in the fields.</td>
</tr>
<tr>
<td>5</td>
<td>Click <strong>Submit</strong>.</td>
</tr>
</tbody>
</table>

---

**Compound Posture Conditions**

Compound conditions are made up of one or more simple conditions, or compound conditions. You can make use of the following compound conditions while defining a Posture policy.

- Compound Conditions—Contains one or more simple conditions, or compound conditions of the type File, Registry, Application, or Service condition
- Antivirus Compound Conditions—Contains one or more AV conditions, or AV compound conditions
- Antispyware Compound Conditions—Contains one or more AS conditions, or AS compound conditions
- Dictionary Compound Conditions—Contains one or more dictionary simple conditions or dictionary compound conditions
- Antimalware Conditions—Contains one or more AM conditions.

**Predefined Condition for Enabling Automatic Updates in Windows Clients**

The pr_AutoUpdateCheck_Rule is a Cisco predefined condition, which is downloaded to the Compound Conditions page. This condition allows you to check whether the automatic updates feature is enabled on Windows clients. If a Windows client fails to meet this requirement, then the Network Access Control (NAC) Agents enforce the Windows client to enable (remediate) the automatic updates feature. After this remediation is done, the Windows client becomes posture compliant. The Windows update remediation that you associate in the posture policy overrides the Windows administrator setting, if the automatic updates feature is not enabled on the Windows client.

**Preconfigured Antivirus and Antispyware Conditions**

Cisco ISE loads preconfigured antivirus and antispyware compound conditions in the AV and AS Compound Condition pages, which are defined in the antivirus and antispyware support charts for Windows and Macintosh operating systems. These compound conditions can check if the specified antivirus and antispyware products exist on all the clients. You can also create new antivirus and antispyware compound conditions in Cisco ISE.
Antivirus and Antispyware Support Chart

Cisco ISE uses an antivirus and antispyware support chart, which provides the latest version and date in the definition files for each vendor product. Users must frequently poll antivirus and antispyware support charts for updates. The antivirus and antispyware vendors frequently update antivirus and antispyware definition files, look for the latest version and date in the definition files for each vendor product.

Each time the antivirus and antispyware support chart is updated to reflect support for new antivirus and antispyware vendors, products, and their releases, the NAC Agents receive a new antivirus and antispyware library. It helps NAC Agents to support newer additions. Once the NAC Agents retrieve this support information, they check the latest definition information from the periodically updated se-checks.xml file (which is published along with the se-rules.xml file in the se-templates.tar.gz archive), and determine whether clients are compliant with the posture policies. Depending upon what is supported by the antivirus and antispyware library for a particular antivirus, or antispyware product, the appropriate requirements will be sent to the NAC Agents for validating their existence, and the status of particular antivirus and antispyware products on the clients during posture validation.

The antivirus and antispyware support chart is available on Cisco.com.

Compliance Module

The compliance module contains a list of fields, such as vendor name, product version, product name, and attributes provided by OPSWAT that supports Cisco ISE posture conditions.

Vendors frequently update the product version and date in the definition files, therefore, you must look for the latest version and date in the definition files for each vendor product by frequently polling the compliance module for updates. Each time the compliance module is updated to reflect the support for new vendors, products, and their releases, the AnyConnect agents receive a new library. It helps AnyConnect agent to support newer additions. Once the AnyConnect agents retrieve this support information, they check the latest definition information from the periodically updated se-checks.xml file (which is published along with the se-rules.xml file in the se-templates.tar.gz archive), and determine whether clients are compliant with the posture policies. Depending upon what is supported by the library for a particular antivirus, antispyware, antimalware, disk encryption, or patch management product, the appropriate requirements will be sent to the AnyConnect agents for validating their existence, and the status of the particular products on the clients during posture validation.

The compliance module is available on Cisco.com.

Table given below lists the OPSWAT API versions that support and do not support the ISE posture policy. There are different policy rules for agents that support versions 3 and 4.

Table 65: OPSWAT API Versions

<table>
<thead>
<tr>
<th>Posture Condition</th>
<th>Compliance Module Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPSWAT</td>
<td></td>
</tr>
<tr>
<td>Antivirus</td>
<td>3.x or earlier</td>
</tr>
<tr>
<td>Antispyware</td>
<td>3.x or earlier</td>
</tr>
<tr>
<td>Antimalware</td>
<td>4.x or later</td>
</tr>
</tbody>
</table>
Create Compound Posture Conditions

You can create compound conditions that can be used in posture policies for posture assessment and validation.

Before you begin
To perform the following task, you must be a Super Admin or Policy Admin.

| Step 1 | Choose Policy > Policy Elements > Conditions > Posture > Compound Conditions > Add. |
| Step 2 | Enter appropriate values for the fields. |
| Step 3 | Click Validate Expression to validate the condition. |
| Step 4 | Click Submit. |

Related Topics
- Posture Conditions, on page 561
- Simple Posture Conditions, on page 561
- Compound Posture Conditions, on page 562
- Predefined Condition for Enabling Automatic Updates in Windows Clients, on page 562

Note
- Be sure to create separate posture policies for version 3.x or earlier and version 4.x or later, in anticipation of clients that may have installed any one of the above versions.
- OESIS version 4 support is provided for compliance module 4.x and Cisco AnyConnect 4.3 and higher. However, AnyConnect 4.3 supports both OESIS version 3 and version 4 policies.
- Version 4 compliance module is supported by ISE 2.1 and higher.

<table>
<thead>
<tr>
<th>Posture Condition</th>
<th>Compliance Module Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk Encryption</td>
<td>3.x or earlier and 4.x or later</td>
</tr>
<tr>
<td>Patch Management</td>
<td>3.x or earlier and 4.x or later</td>
</tr>
<tr>
<td>USB</td>
<td>4.x or later</td>
</tr>
<tr>
<td>Non-OPSWAT File</td>
<td>Any version</td>
</tr>
<tr>
<td>Non-OPSWAT Application</td>
<td>Any version</td>
</tr>
<tr>
<td>Non-OPSWAT Compound</td>
<td>Any version</td>
</tr>
<tr>
<td>Non-OPSWAT Registry</td>
<td>Any version</td>
</tr>
<tr>
<td>Non-OPSWAT Service</td>
<td>Any version</td>
</tr>
</tbody>
</table>
Create Patch Management Conditions

You can create a policy to check the status of a selected vendor’s patch management product. For example, you can create a condition to check if Microsoft System Center Configuration Manager (SCCM), Client Version 4.x software product is installed at an endpoint.

**Note**

Supported versions of Cisco ISE and AnyConnect:

- Cisco ISE version 1.4 and later
- AnyConnect version 4.1 and later

**Before you begin**

To perform the following task, you must be a Super Admin or Policy Admin.

**Step 1** Choose Policy > Policy Elements > Conditions > Posture > Patch Management Condition.

**Step 2** Click Add.

**Step 3** Enter the condition name and description in the Name and Description fields.

**Step 4** Choose the appropriate operating system from the Operating System drop-down field.

**Step 5** Choose the Compliance Module from the drop-down list.

**Step 6** Choose the Vendor Name from the drop-down list.

**Step 7** Choose the Check Type.

**Step 8** Choose the appropriate patch from the Check patches installed drop-down list.

**Step 9** Click Submit.

**Related Topics**

- Patch Management Condition Settings, on page 1110
- Add a Patch Management Remediation, on page 793

Create Disk Encryption Conditions

You can create a policy to check if an end point is compliant with the specified data encryption software. For example, you can create a condition to check if the C: drive is encrypted in an endpoint. If the C: drive is not encrypted then the end point receives a non-compliance notification and ISE logs a message.

**Before you begin**

To perform the following task, you must be a Super Admin or Policy Admin. You can associate a Disk Encryption condition with a posture requirement only when you use the AnyConnect ISE posture agent.
Configure Posture Policies

A posture policy is a collection of posture requirements that are associated with one or more identity groups, and operating systems. The Dictionary Attributes are optional conditions that can be used along with the identity groups and the operating systems to define different policies for the clients.

See Posture Services on the Cisco ISE Configuration Guide for more information.

Before you begin

- You must have an understanding of the AUP.
- You must have an understanding of periodic reassessments (PRA).

Step 1: Choose Policy > Posture or Work Centers > Posture > Posture Policy.
Step 2: From the Rule Status drop-down list, choose either Enabled or Disabled.
Step 3: In the Rule Name field, enter the name of the policy.
Note: It is a best practice to configure a posture policy with each requirement as a separate rule in order to avoid unexpected results.

Step 4: From the Identity Groups column, select the required identity group.
To create posture policies based on end-point identity groups, select Endpoint Identity Groups from the Identity Groups column.

Step 5: From the Operating Systems column, select the operating system.

Step 6: From the Compliance Module column, select the required compliance module:

- 4.x or Later—Supports antimalware, disk encryption, patch management, and USB conditions.
- 3.x or Earlier—Supports antivirus, antisyware, disk encryption, and patch management conditions
- Any Version—Supports file, service, registry, application, and compound conditions.

Step 7: From the Posture Type column, select the Posture Type.

- AnyConnect—Deploys the AnyConnect agent to monitor and enforce Cisco ISE policies that require client interaction.
- AnyConnect Stealth—Deploys the AnyConnect agent to monitor and enforce Cisco ISE posture policies without any client interaction.
• **Temporal Agent**—A temporary executable file that is run on the client to check the compliance status.

**Step 8**  
In **Other Conditions**, you can add one or more dictionary attributes and save them as simple or compound conditions to a dictionary.  

**Note**  
Dictionary simple conditions and dictionary compound conditions that you create in the Posture Policy page are not displayed while configuring an authorization policy.

**Step 9**  
Specify the requirements in the **Requirements** field.  

**Step 10**  
Click **Save**.

---

**Related Topics**

- Create Client Posture Requirements, on page 797  
- Configure Periodic Reassessments, on page 778

---

**Prerequisite for Certificate-Based Conditions**

Client Provisioning and Posture Policy rules may include conditions based on certificate attributes. A prerequisite for certificate-based conditions in either the Client Provisioning or Posture Policy is to ensure that there is a matching Authorization Policy rule based on the same certificate attribute.

For example, you should use the same attribute as shown in the figures, the Issuer – Common Name attribute is used in both Client Provisioning or posture and authorization policies.

*Figure 54: Cisco Provisioning Policy*
ISE server certificate must be trusted in the System Certificate store for AnyConnect 4.6 MR2 and above. Any posture check or remediation that requires elevated privileges will not work if the server is untrusted.

- Windows OS—The server certificate must be added to the System Certificate store.
- MAC OS—The server certificate must be added to the System Keychain. It is recommended that you use the command-line utility to trust the certificate. Adding the certificate to the System Keychain using the Keychain Access app might not work if it is already present in the Login Keychain.

### Default Posture Policies

The Cisco ISE software comes with a number of pre-configured posture policies (Policy > Posture) that make it easier for you to create the posture policies and profiles. These policies are disabled by default. You can enable these policies based on your requirements. Listed below are some of the default posture policies.

<table>
<thead>
<tr>
<th>Rule Name</th>
<th>Description</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default_Antimalware_Policy_Mac</td>
<td>Checks if endpoints have any of the supported vendor’s antimalware software (that is recognized by AnyConnect) installed and running in their devices.</td>
<td>Any_AM_Installation</td>
</tr>
<tr>
<td>Default_Antimalware_Policy_Win</td>
<td>Checks if endpoints have any of the supported vendor’s antimalware software (that is recognized by AnyConnect) installed and running in their devices.</td>
<td>Any_AM_Installation_Win</td>
</tr>
<tr>
<td>Default_AppVis_Policy_Mac</td>
<td>Gathers information and reports all the applications that are installed on a given endpoint.</td>
<td>Default_AppVis_Requirement_Mac</td>
</tr>
<tr>
<td>Default_AppVis_Policy_Win</td>
<td>Gathers information and reports all the applications that are installed on a given endpoint.</td>
<td>Default_AppVis_Requirement_Win</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Description</td>
<td>Requirements</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Default_Firewall_Policy_Mac</td>
<td>Checks if endpoints have any of the supported vendor’s Firewall program (that is recognized by AnyConnect) installed.</td>
<td>Default_Firewall_Requirement_Mac</td>
</tr>
<tr>
<td>Default_Firewall_Policy_Win</td>
<td>Checks if endpoints have any of the supported vendor’s Firewall program (that is recognized by AnyConnect) installed.</td>
<td>Default_Firewall_Requirement_Win</td>
</tr>
<tr>
<td>Default_USB_Block_Win</td>
<td>Ensures that the endpoint device does not have any USB storage devices connected.</td>
<td>USB_Block</td>
</tr>
</tbody>
</table>

### Posture Assessment Options

The following table provides a list of posture assessment (posture conditions) options that are supported by the ISE Posture Agents for Windows and Macintosh, and the Web Agent for Windows.

**Table 66: Posture Assessment Options**

<table>
<thead>
<tr>
<th>ISE Posture Agent for Windows</th>
<th>Cisco Temporal Agent for Windows</th>
<th>ISE Posture Agent for Macintosh OS X</th>
<th>Cisco Temporal Agent for Macintosh OS X</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Operating System/Service Packs/Hotfixes</td>
<td>Service Check (Temporal agent 4.5 and ISE 2.3)</td>
<td>Service Check (AC 4.1 and ISE 1.4)</td>
</tr>
<tr>
<td>Service Check</td>
<td>Registry Check (Temporal agent 4.5 and ISE 2.3)</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Registry Check</td>
<td>File Check (Temporal agent 4.5 and ISE 2.3)</td>
<td>File Check (AC 4.1 and ISE 1.4)</td>
<td>File Check (Temporal agent 4.5 and ISE 2.3)</td>
</tr>
<tr>
<td>File Check</td>
<td>Application Check (Temporal agent 4.5 and ISE 2.3)</td>
<td>Application Check (AC 4.1 and ISE 1.4)</td>
<td>Application Check (Temporal agent 4.5 and ISE 2.3)</td>
</tr>
<tr>
<td>Application Check</td>
<td>Antimalware Installation</td>
<td>Antimalware Installation</td>
<td>Antimalware Installation</td>
</tr>
<tr>
<td>Antivirus Installation</td>
<td>Antivirus Version/ Antivirus Definition Date</td>
<td>Antivirus Version/ Antivirus Definition Date</td>
<td>Antivirus Version/ Antivirus Definition Date</td>
</tr>
<tr>
<td>Antivirus Version/ Antivirus Definition Date</td>
<td>OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported</td>
<td>OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported</td>
<td></td>
</tr>
</tbody>
</table>
Posture Remediation Options

The following table provides a list of posture remediation options that are supported by the ISE Posture Agents for Windows and Macintosh, and the Web Agent for Windows.

Table 67: Posture Remediation Options

<table>
<thead>
<tr>
<th>ISE Posture Agent for Windows</th>
<th>Cisco Temporal Agent for Windows</th>
<th>ISE Posture Agent for Macintosh OS X</th>
<th>Cisco Temporal Agent for Macintosh OS X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antispyware Installation</td>
<td>OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported</td>
<td>Antispyware Installation</td>
<td>OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported</td>
</tr>
<tr>
<td>Antispyware Version/Antispyware Definition Date</td>
<td>OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported</td>
<td>Antispyware Version/Antispyware Definition Date</td>
<td>OPSWAT version 4 is used, hence no Antivirus/Antispyware support; only Antimalware is supported</td>
</tr>
<tr>
<td>Patch Management Check (AC 4.1 and ISE 1.4)</td>
<td>Only Patch Management installation check</td>
<td>Patch Management Check (AC 4.1 and ISE 1.4)</td>
<td>—</td>
</tr>
<tr>
<td>Windows Update Running</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Windows Update Configuration</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>WSUS Compliance Settings</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>
**Custom Conditions for Posture**

A posture condition can be any one of the following simple conditions: a file, a registry, an application, a service, or a dictionary condition. One or more conditions from these simple conditions form a compound condition, which can be associated with a posture requirement.

After an initial posture update, Cisco ISE also creates Cisco-defined simple and compound conditions. Cisco-defined simple conditions use the pc_as and compound conditions use pr_as.

A user-defined condition or a Cisco-defined condition includes both simple and compound conditions.

Posture service makes use of internal checks based on antivirus and antispyware (AV/AS) compound conditions. Hence, posture reports do not reflect the exact AV/AS compound-condition names that you have created. The reports display only the internal check names of AV/AS compound conditions.

For example, if you have created an AV compound condition named "MyCondition_AV_Check" to check any Vendor and any Product, the posture reports will display the internal check, that is “av_def_ANY”, as the condition name, instead of "MyCondition_AV_Check".

**Posture End-Point Custom Attributes**

You can use the posture endpoint custom attributes to create client provisioninging and posture policies. You can create a maximum of 100 endpoint custom attributes. The following types of endpoint custom attributes are supported: Int, String, Long, Boolean, Float, IP, and Date.

Endpoint custom attributes can be used to white list or black list devices based on certain attributes or to assign certain privileges based on the posture or client provisioning polices.

**Create Posture Policy Using End-Point Custom Attributes**

To create a posture policy using endpoint custom attributes:

**Step 1**
Create the endpoint custom attributes.

a) Choose **Administration > Identity Management > Settings > Endpoint Custom Attributes**.

b) Enter the **Attribute Name** (for example, deviceType) and Data Type (for example, String) in the **Endpoint Custom Attributes** area.

c) Click **Save**.
Step 2 Assign values to the custom attributes.
   a) Choose **Context Visibility > Endpoints**.
   b) Assign the custom attribute values.
      • Check the required MAC address check box, and then click **Edit**.
      • Or, click the required MAC address, and then click **Edit** in the **Endpoints** page.
   c) Ensure that the custom attribute that you created is displayed in the **CustomAttributes** area in the **Edit Endpoint** dialog box.
   d) Click **Edit** and enter the required attribute value (for example, deviceType = Apple-iPhone).
   e) Click **Save**.

Step 3 Create a posture policy using the custom attributes and values.
   a) Choose **Work Centers > Posture > Posture Policy**.
   b) Create the required policy. Choose the custom attributes by clicking **Other Conditions** and select the required dictionary (for example, choose **Endpoints > deviceType**, the custom attribute that you created in Step 1). For more information, see the Cisco Temporal Agent Workflow, on page 804.
   c) Click **Save**.

---

To create a client provisioning policy using endpoint custom attributes:

1. Choose **Work Centers > Posture > Client Provisioning > Client Provisioning Policy**.
2. Create the required policy.
   • Create the required rule (for example, Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117).
   • Choose the custom attributes by clicking **Other Conditions** and selecting the required dictionary.

---

**Custom Posture Remediation Actions**

A custom posture remediation action is a file, a link, an antivirus or antispyware definition updates, launching programs, Windows updates, or Windows Server Update Services (WSUS) remediation types.

**Related Topics**

Add a File Remediation, on page 793
Add a Link Remediation, on page 793
Add an Antivirus Remediation, on page 794
Add an Antispyware Remediation, on page 794
Add a Launch Program Remediation, on page 795
Add a Windows Update Remediation, on page 795
Add a Windows Server Update Services Remediation, on page 796
Add a Patch Management Remediation, on page 793
Add a File Remediation

A file remediation allows clients to download the required file version for compliance. The client agent remediates an endpoint with a file that is required by the client for compliance.

You can filter, view, add, or delete file remediations in the File Remediations page, but you cannot edit file remediations. The File Remediations page displays all the file remediations along with their name and description and the files that are required for remediation.

Step 1  Choose Policy > Policy Elements > Results > Posture.
Step 2  Click Remediation Actions.
Step 3  Click File Remediation.
Step 4  Click Add.
Step 5  Enter the name and description of the file remediation in the Name and Description fields.
Step 6  Modify the values in the New File Remediation page.
Step 7  Click Submit.

Add a Link Remediation

A link remediation allows clients to click a URL to access a remediation page or resource. The client agent opens a browser with the link and allow the clients to remediate themselves for compliance.

The Link Remediation page displays all the link remediations along with their name and description and their modes of remediation.

Step 1  Choose Policy > Policy Elements > Results > Posture.
Step 2  Click Remediation Actions.
Step 3  Click Link Remediation.
Step 4  Click Add.
Step 5  Modify the values in the New Link Remediation page.
Step 6  Click Submit.

Add a Patch Management Remediation

You can create a patch management remediation, which updates clients with up-to-date file definitions for compliance after remediation.

The Patch Management Remediation page displays the remediation type, patch management vendor names, and various remediation options.

Step 1  Choose Policy > Policy Elements > Results > Posture.
Step 2  Click Remediation Actions.
Add an Antivirus Remediation

You can create an antivirus remediation, which updates clients with up-to-date file definitions for compliance after remediation.

The AV Remediations page displays all the antivirus remediations along with their name and description and their modes of remediation.

Add an Antispyware Remediation

You can create an antispyware remediation, which updates clients with up-to-date file definitions for compliance after remediation.

The AS Remediations page displays all the antivirus remediations along with their name and description and their modes of remediation.
Add a Launch Program Remediation

You can create a launch program remediation, where the client agent remediates clients by launching one or more applications for compliance.

The Launch Program Remediations page displays all the launch program remediations along with their name and description and their modes of remediation.

Step 1  Choose Policy > Policy Elements > Results > Posture.
Step 2  Click Remediation Actions.
Step 3  Click Launch Program Remediation.
Step 4  Click Add.
Step 5  Modify the values in the New Launch Program Remediation page.
Step 6  Click Submit.

Troubleshoot Launch Program Remediation

Problem
When an application is launched as a remediation using Launch Program Remediation, the application is successfully launched (observed in the Windows Task Manager), however, the application UI is not visible.

Solution
The Launch program UI application runs with system privileges, and is visible in the Interactive Service Detection (ISD) window. To view the Launch program UI application, ISD should be enabled for the following OS:

- Windows Vista: ISD is in stop state by default. Enable ISD by starting ISD service in services.msc.
- Windows 7: ISD service is enabled by default.
- Windows 8/8.1: Enable ISD by changing "NoInteractiveServices" from 1 to 0 in the registry: \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Windows.

Add a Windows Update Remediation

The Windows Update Remediations page displays all the Windows update remediations along with their name and description and their modes of remediation.

Step 1  Choose Policy > Policy Elements > Results > Posture.
Step 2  Click Remediation Actions.
Step 3  Click Windows Update Remediation.
Step 4  Click Add.
Step 5  Modify the values in the New Windows Update Remediation page.
Add a Windows Server Update Services Remediation

You can configure Windows clients to receive the latest WSUS updates from a locally administered or a Microsoft-managed WSUS server for compliance. A Windows Server Update Services (WSUS) remediation installs latest Windows service packs, hotfixes, and patches from a locally managed WSUS server or a Microsoft-managed WSUS server.

You can create a WSUS remediation where the client agent integrates with the local WSUS Agent to check whether the endpoint is up-to-date for WSUS updates.

Posture Assessment Requirements

A posture requirement is a set of compound conditions with an associated remediation action that can be linked with a role and an operating system. All the clients connecting to your network must meet mandatory requirements during posture evaluation to become compliant on the network.

Posture-policy requirements can be set to mandatory, optional, or audit types in posture policies. If requirements are optional and clients fail these requirements, then the clients have an option to continue during posture evaluation of endpoints.

**Mandatory Requirements**

During policy evaluation, the agent provides remediation options to clients who fail to meet the mandatory requirements defined in the posture policy. End users must remediate to meet the requirements within the time specified in the remediation timer settings.
For example, you have specified a mandatory requirement with a user-defined condition to check the existence of C:\temp\text.file in the absolute path. If the file does not exist, the mandatory requirement fails and the user will be moved to Non-Compliant state.

**Optional Requirements**

During policy evaluation, the agent provides an option to clients to continue, when they fail to meet the optional requirements specified in the posture policy. End users are allowed to skip the specified optional requirements.

For example, you have specified an optional requirement with a user-defined condition to check for an application running on the client machine, such as Calc.exe. Although, the client fails to meet the condition, the agent prompts an option to continue further so that the optional requirement is skipped and the end user is moved to Compliant state.

**Audit Requirements**

Audit requirements are specified for internal purposes and the agent does not prompt any message or input from end users, regardless of the pass or fail status during policy evaluation.

For example, you are in the process of creating a mandatory policy condition to check if end users have the latest version of the antivirus program. If you want to find out the non-compliant end users before actually enforcing it as a policy condition, you can specify it as an audit requirement.

**Visibility Requirements**

During policy evaluation, the agent reports compliance data for visibility requirements, every 5 to 10 minutes.

### Client System Stuck in Noncompliant State

If a client machine is unable to remediate a mandatory requirement, the posture status changes to “noncompliant” and the agent session is quarantined. To get the client machine past this “noncompliant” state, you need to restart the posture session so that the agent starts posture assessment on the client machine again. You can restart the posture session as follows:

- In wired and wireless Change of Authorization (CoA) in an 802.1X environment:
  - You can configure the Reauthentication timer for a specific authorization policy when you create a new authorization profile in the New Authorization Profiles page. “Configuring Permissions for Downloadable ACLs” section on page 20-11 for more information.
  - Wired users can get out of the quarantine state once they disconnect and reconnect to the network. In a wireless environment, the user must disconnect from the wireless lan controller (WLC) and wait until the user idle timeout period has expired before attempting to reconnect to the network.

- In a VPN environment—Disconnect and reconnect the VPN tunnel.

### Create Client Posture Requirements

You can create a requirement in the Requirements page where you can associate user-defined conditions and Cisco defined conditions, and remediation actions. Once created and saved in the Requirements page, user-defined conditions and remediation actions can be viewed from their respective list pages.
Before you begin

- You must have an understanding of acceptable use policies (AUPs) for a posture.

---

**Step 1** Choose Policy > Policy Elements > Results > Posture > Requirements.

**Step 2** Enter the values in the Requirements page.

**Step 3** Click Done to save the posture requirement in read-only mode.

**Step 4** Click Save.

---

**Related Topics**

- Client System Stuck in Noncompliant State, on page 797
- Posture Assessment Requirements, on page 796

---

**Custom Permissions for Posture**

A custom permission is a standard authorization profile that you define in Cisco ISE. Standard authorization profiles set access privileges based on the matching compliance status of the endpoints. The posture service broadly classifies the posture into unknown, compliant, and noncompliant profiles. The posture policies and the posture requirements determine the compliance status of the endpoint.

You must create three different authorization profiles for an unknown, compliant, and noncompliant posture status of endpoints that can have different set of VLANs, DACLs and other attribute value pairs. These profiles can be associated with three different authorization policies. To differentiate these authorization policies, you can use the Session:PostureStatus attribute along with other conditions.

**Unknown Profile**

If no matching posture policy is defined for an endpoint, then the posture compliance status of the endpoint may be set to unknown. A posture compliance status of unknown can also apply to an endpoint where a matching posture policy is enabled but posture assessment has not yet occurred for that endpoint and, therefore no compliance report has been provided by the client agent.

**Compliant Profile**

If a matching posture policy is defined for an endpoint, then the posture compliance status of the endpoint is set to compliant. When the posture assessment occurs, the endpoint meets all the mandatory requirements that are defined in the matching posture policy. For an endpoint that is postured compliant, it can be granted privileged network access on your network.

**Noncompliant Profile**

The posture compliance status of an endpoint is set to noncompliant when a matching posture policy is defined for that endpoint but it fails to meet all the mandatory requirements during posture assessment. An endpoint that is postured noncompliant matches a posture requirement with a remediation action, and it should be granted limited network access to remediation resources in order to remediate itself.
Configure Standard Authorization Policies

You can define two types of authorization policies on the Authorization Policy page, standard exceptions and standard authorization policies. The standard authorization policies that are specific to posture are used to make policy decisions based on the compliance status of endpoints.

**Step 1** Choose **Policy > Policy Sets**.

**Step 2** In the **View** column, click the arrow icon adjacent the corresponding Default Policy.

**Step 3** In the **Actions** column, click the cog icon, and then from the dropdown list, choose a new authorization policy. A new row appears in the **Policy Sets** table.

**Step 4** Enter a rule name.

**Step 5** From the **Conditions** column, click the (+) symbol.

**Step 6** Create the required conditions on the **Conditions Studio Page**. In the **Editor** section, click the **Click To Add an Attribute** text box, and select the required Dictionary and Attribute.

You can drag and drop a Library condition to the **Click To Add An Attribute** text box.

**Step 7** Click **Use** to create a new standard authorization policy in read-only mode.

**Step 8** Click **Save**.

Best Practices for Network Drive Mapping with Posture

During posture assessment of a Windows endpoint, the endpoint user may encounter a delay in accessing the desktop. This may be due to Windows trying to restore the file server drive letter mappings before providing the user access to the desktop. The best practices to avoid the delay during posture are:

- Endpoints should be able to reach the Active Directory server because the file server drive letter cannot be mapped without reaching the AD. When posture (with AnyConnect ISE posture agent) triggers, it blocks access to AD, causing delay in login. Use Posture Remediation ACLs to provide access to AD servers before posture is completed.

- You should set a delay for the login script until posture completes and then you have to set the Persistence attribute to NO. Windows tries to reconnect all the network drives during login and this cannot be done until AnyConnect ISE posture agent gains full network access.

AnyConnect Stealth Mode Workflow

The process of configuring AnyConnect in the stealth mode involves a series of steps. You should perform the following steps in Cisco ISE.

**Step 1** Create an AnyConnect agent profile, see Create an AnyConnect Agent Profile.

**Step 2** Create an AnyConnect Configuration for AnyConnect Packages, see Create an AnyConnect Configuration for AnyConnect Packages.
Create an AnyConnect Agent Profile

Before you begin
You must upload the AnyConnect Cisco packages for MAC and Windows OS and the AnyConnect compliance modules.

Step 1 Choose Policy > Policy Elements > Results > Client Provisioning > Resources page.
Step 2 From the Add drop-down list, choose Nac Agent or AnyConnect Posture Profile.
Step 3 From the Posture Agent Profile Settings drop-down list, choose AnyConnect.
Step 4 In the Name field, type the required name (for example, AC_Agent_Profile).
Step 5 In the Agent Behavior section, select the Stealth Mode parameter as Enabled.
Step 6 Click Save.

What to do next
You should create the AnyConnect configuration for the AnyConnect packages.

Create an AnyConnect Configuration for AnyConnect Packages

Step 1 Navigate to the Policy > Policy Elements > Results > Client Provisioning > Resources page.
Step 2 From the Add drop-down list, choose AnyConnect Configuration.
Step 3 From the Select AnyConnect Package drop-down list, choose the required AnyConnect package (for example, AnyConnectDesktopWindows 4.4.117.0).
Step 4 In the Configuration Name text box, type the required Name (for example, AC_Win_44117).
Step 5 In the Compliance Module drop-down list, choose the required compliance module (for example, AnyConnectComplianceModuleWindows 4.2.437.0).
Step 6 In the AnyConnect Module Selection section, check the ISE Posture and Network Access Manager check boxes.
Step 7 In the Profile Selection section, from the ISE Posture drop-down list, choose the AnyConnect agent profile (for example, AC_Agent_Profile).
Step 8 From the Network Access Manager drop-down list, choose the required AnyConnect agent profile (for example, AC_Agent_Profile).
What to do next
You should upload the Open DNS profile to be pushed to the client.

Upload a Open DNS Profile in Cisco ISE

The Open DNS profile is pushed to the client.

**Step 1** Navigate to the Policy > Policy Elements > Results > Client Provisioning > Resources page.

**Step 2** From the Add drop-down list, choose Agent Resources From Local Disk.

**Step 3** From the Category drop-down list, choose Customer Created Packages.

**Step 4** From the Type drop-down list, choose AnyConnect Profile.

**Step 5** In the Name text box, type the required name (for example, OpenDNS).

**Step 6** Click Browse and locate the JSON file from the local disk.

**Step 7** Click Submit.

What to do next
You should create the client provisioning policy.

Create a Client Provisioning Policy

**Step 1** Navigate to the Policy > Client Provisioning page.

**Step 2** Create the required rule (for example, Rule Name=WindowsAll, if Identity Groups=Any and Operating Systems=Windows All and Other Conditions=Conditions, then Results=AC_Win_44117).

What to do next
You should create the posture condition.

Create a Posture Condition

**Step 1** Navigate to the Policy > Policy Elements > Conditions > Posture > File Condition.

**Step 2** Enter the required name (for example, filechk).

**Step 3** From the Operating Systems drop-down list, choose Windows 7 (All).

**Step 4** From the File Type drop-down list, choose FileExistence.

**Step 5** From the File Path drop-down list, choose ABSOLUTE_PATH C:\test.txt.

**Step 6** From the File Operator drop-down list, choose DoesNotExist.
Create Posture Remediation

The file condition checks if test.txt file exists on the endpoint. If it does not exist, the remediation is to block the USB port and prevent the installation of the file using a USB device.

**Step 1** Navigate to the **Policy > Policy Elements > Results > Remediation Actions > USB Remediations** page.

**Step 2** Enter the required name (for example, clientless_mode_block).

**Step 3** Click **Submit**.

Create Posture Requirement in Stealth Mode

When you create a Remediation action from the Requirements page, only the remediations that are applicable to stealth mode are displayed: Anti-Malware, Launch Program, Patch Management, USB, Windows Server Update Services, and Windows Update.

**Step 1** Navigate to the **Policy > Policy Elements > Results > Client Provisioning > Resources** page.

**Step 2** Create the required posture requirement (for example, Name=win7Req for Operating Systems=Windows7(All) using Compliance Module=4.x or later using Posture Type=AnyConnect Stealth met if Condition=filechk then Remediation Actions=clientless_mode_block).

Create Posture Policy

**Before you begin**

Ensure that the posture policy requirement and the policy are created in the clientless mode.

**Step 1** Choose **Policy > Posture**.

**Step 2** Create the required rule. For example, if Identity Groups=Any and Operating Systems=Windows 7(All) and Compliance Module=4.x or later and Posture Type=AnyConnect Stealth then Requirements=win7Req.
Note For Client Provisioning without URL redirection, configuring the conditions with attributes specific to Network Access or Radius will not work and matching of the client provisioning policy might fail due to the non-availability of session information for the specific user in the Cisco ISE server. However, Cisco ISE allows configuring conditions for the externally added identity groups.

---

Posture Types

There are three posture types that can be used monitor and enforce Cisco ISE posture policies:

- **AnyConnect**—Deploys the AnyConnect agent to monitor and enforce Cisco ISE posture policies that require client interaction.

- **AnyConnect Stealth**— Runs posture as a service without any user interaction.

- **Temporal Agent**—A temporary executable file that you can configure in the Cisco ISE GUI to run on the client. When a client attempts to access the trusted network, Cisco ISE pushes the executable file that the user has to run on the client. The temporal agent checks the compliance status again and sends the status to Cisco ISE, which in turn takes the required action based on the results. The temporal agent is removed from the client when compliance processing is completed. The temporal agent does not support custom remediation. The default remediation supports only message text.

  Note

  - You can configure posture policies using the Posture Types as Temporal Agent and Compliance Module as 4.x or later. While creating the remediation and requirements for such policies, ensure that you do not change the compliance module to “3.x or earlier” or “Any Version”.

  - For the Temporal Agent, you can only view Patch Management conditions containing the Installation check type in the Requirements page.

  - Cisco ISE does not support VLAN-controlled posture environment using the Temporal Agent for Mac OSX. This is because when you change the network access from an existing VLAN to a new VLAN, the user’s IP address must be released before the VLAN change, and a new IP address must be requested through DHCP when the user connects to the new VLAN. This requires root privileges but the Temporal Agent runs as a user process.

Cisco ISE supports ACL-controlled posture environment, which does not require the refreshing of endpoint IP addresses.

Conditions Unsupported by the Temporal Agent:

- **Service Condition MAC**—System Daemon check

- **Service Condition-MAC**—Daemon or User Agent check

- **PM**—Up To Date check

- **PM**—Enabled check
• DE—Encryption check

The Client Provisioning page (Policy > Policy Elements > Results > Client Provisioning > Resources) and
the Posture Requirements page (Policy > Policy Elements > Results > Posture > Requirements) contains the
posture types, and the recommended best practice is to provision the posture profile in the Client Provisioning
page.

When you choose the AnyConnect Stealth posture type in the posture requirement, some of the conditions,
remediations, or attributes in a condition are disabled (grayed out). For example, when you enable AnyConnect
Stealth requirement, the Manual Remediation Type is disabled (grayed out) because this action requires
client-side interaction.

Mapping the posture profile to the AnyConnect configuration, and then mapping the Anyconnect configuration
to the Client Provisioning page for AnyConnect stealth mode deployment supports:

• AnyConnect to read the posture profile and set it to the intended mode.

• AnyConnect to send information related to the selected mode to Cisco ISE during initial posture request.

• Cisco ISE to match the right policy, based on the mode and other factors, such as identity group, OS,
and compliance module.

---

Note

AnyConnect version 4.4 and later support Cisco ISE posture in Stealth mode.

Related Topics

AnyConnect Stealth Mode Workflow, on page 799
Cisco Temporal Agent Workflow, on page 804

Cisco Temporal Agent Workflow

The process of configuring the Cisco temporal agent involves a series of steps. You should perform the
following steps in Cisco ISE.

Step 1 Create Posture Condition
Step 2 Create Posture Requirements
Step 3 Create the Posture Policy
Step 4 Configure the Client Provisioning Policy
Step 5 Download and Launch Cisco Temporal Agent

Create Posture Condition

Step 1 Navigate to the Policy > Policy Elements > Conditions > Posture > File Condition.
Step 2 Enter the required name (for example, filecondwin).
Create Posture Requirements

Step 1 Choose Policy > Policy Elements > Results > Posture > Requirements
Step 2 From the Edit drop-down list, choose Insert New Requirement.
Step 3 Enter the Name, Operating Systems, and Compliance Module (for example, Name filereqwin, Operating Systems Windows All, Compliance Module 4.x or later).
Step 4 In the Posture Type drop-down, choose Temporal Agent.
Step 5 Select the required condition (for example, filecondwin).
Note For the Cisco Temporal Agent, you can only view Patch Management conditions containing the Installation check type in the Requirements page.
Step 6 Select the Message Text Only remediation action.
Note The temporal agent is supported by AnyConnect 4.x or later.

Configure the Client Provisioning Policy

Step 1 Choose Policy > Client Provisioning.
Step 2 Create the required rule (for example, Rule Name=Win, Identity Groups=Any, Operating Systems=Windows All, Other Conditions=Conditions, Results=CiscoTemporalAgentWindows4.5).
## Download and Launch Cisco Temporal Agent

| Step 1 | Connect to the SSID. |
| Step 2 | Launch a Browser and you will be redirected to the Client Provisioning Portal. |
| Step 3 | Click **Start**. This checks if the Cisco Temporal agent is installed and running. |
| Step 4 | Click **This Is My First Time Here**. |
| Step 5 | Choose **Click Here to Download and Launch Cisco Temporal Agent**. |
| Step 6 | Save the Cisco Temporal Agent .exe or .dmg file for Windows or Mac OS X respectively. For Windows, run the .exe file and for Mac OS X, double-click the .dmg file and run the acisetempagent app. The Cisco Temporal Agent scans the client and displays the results, such as Red cross marks for non-compliant checks. |
Cisco TrustSec Policies Configuration

- TrustSec Architecture, on page 807
- Integration with Cisco Digital Network Architecture Center (DNA-C), on page 810
- TrustSec Dashboard, on page 811
- Configure TrustSec Global Settings, on page 814
- Configure TrustSec Matrix Settings, on page 815
- Configure TrustSec Devices, on page 815
- Configure TrustSec AAA Servers, on page 817
- Security Groups Configuration, on page 818
- Egress Policy, on page 823
- SGT Assignment, on page 837
- TrustSec Configuration and Policy Push, on page 839
- Security Group Tag Exchange Protocol, on page 847
- Add an SXP Domain Filter, on page 849
- Configure SXP Settings, on page 850
- TrustSec-ACI Integration, on page 850
- Configure ACI Settings, on page 851
- Run Top N RBACL Drops by User Report, on page 852

TrustSec Architecture

The Cisco TrustSec solution establishes clouds of trusted network devices to build secure networks. Each device in the Cisco TrustSec cloud is authenticated by its neighbors (peers). Communication between the devices in the TrustSec cloud is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanisms. The TrustSec solution uses the device and user identity information that it obtains during authentication to classify, or color, the packets as they enter the network. This packet classification is maintained by tagging packets when they enter the TrustSec network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows Cisco ISE to enforce access control policies by enabling the endpoint device to act upon the SGT to filter traffic.

The following figure shows an example of a TrustSec network cloud.
**TrustSec Components**

The key TrustSec components include:

- **Network Device Admission Control (NDAC)**—In a trusted network, during authentication, each network device (for example Ethernet switch) in a TrustSec cloud is verified for its credential and trustworthiness by its peer device. NDAC uses the IEEE 802.1X port-based authentication and uses Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) as its Extensible Authentication Protocol (EAP) method. Successful authentication and authorization in the NDAC process results in Security Association Protocol negotiation for IEEE 802.1AE encryption.

- **Endpoint Admission Control (EAC)**—An authentication process for an endpoint user or a device connecting to the TrustSec cloud. EAC typically happens at the access level switch. Successful authentication and authorization in EAC process results in SGT assignment to the user or device. EAC access methods for authentication and authorization includes:
  - 802.1X port-based authentication
• MAC authentication bypass (MAB)
• Web authentication (WebAuth)

• Security Group (SG)—A grouping of users, endpoint devices, and resources that share access control policies. SGs are defined by the administrator in Cisco ISE. As new users and devices are added to the TrustSec domain, Cisco ISE assigns these new entities to the appropriate security groups.

• Security Group Tag (SGT)—TrustSec service assigns to each security group a unique 16-bit security group number whose scope is global within a TrustSec domain. The number of security groups in the switch is limited to the number of authenticated network entities. You do not have to manually configure security group numbers. They are automatically generated, but you have the option to reserve a range of SGTs for IP-to-SGT mapping.

• Security Group Access Control List (SGACL)—SGACLs allow you to control the access and permissions based on the SGTs that are assigned. The grouping of permissions into a role simplifies the management of security policy. As you add devices, you simply assign one or more security groups, and they immediately receive the appropriate permissions. You can modify the security groups to introduce new privileges or restrict current permissions.

• Security Exchange Protocol (SXP)—SGT Exchange Protocol (SXP) is a protocol developed for TrustSec service to propagate the IP-SGT bindings across network devices that do not have SGT-capable hardware support to hardware that supports SGT/SGACL.

• Environment Data Download—The TrustSec device obtains its environment data from Cisco ISE when it first joins a trusted network. You can also manually configure some of the data on the device. The device must refresh the environment data before it expires. The TrustSec device obtains the following environment data from Cisco ISE:
  • Server lists—List of servers that the client can use for future RADIUS requests (for both authentication and authorization)
  • Device SG—Security group to which the device itself belongs
  • Expiry timeout—Interval that controls how often the TrustSec device should download or refresh its environment data

• Identity-to-Port Mapping—A method for a switch to define the identity on a port to which an endpoint is connected, and to use this identity to look up a particular SGT value in the Cisco ISE server.

### TrustSec Terminology

The following table lists some of the common terms that are used in the TrustSec solution and their meaning in an TrustSec environment.

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supplicant</td>
<td>A device that tries to join a trusted network.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The process of verifying the identity of each device before allowing it to be part of the trusted network.</td>
</tr>
</tbody>
</table>
### Supported Switches and Required Components for TrustSec

To set up a Cisco ISE network that is enabled with the Cisco TrustSec solution, you need switches that support the TrustSec solution and other components. Apart from the switches, you also need other components for identity-based user access control using the IEEE 802.1X protocol. For a complete up-to-date list of the Trustsec-supported Cisco switch platforms and the required components, see Cisco TrustSec-Enabled Infrastructure.

### Integration with Cisco Digital Network Architecture Center (DNA-C)

Cisco ISE is a major component of Cisco’s Digital Network Architecture (DNA). Cisco DNA allows you to automate your network to provide business agility. Cisco ISE provides Cisco DNA with policy components
that segment your network to help mitigate security threats and vulnerabilities. When Cisco ISE and Cisco DNA are integrated, Cisco ISE provides groups and policies to Cisco DNA. You can create policies in Cisco DNA-C or in Cisco ISE. DNA uses these policies to enforce controlled network access

**Enabling DNA to Connect to ISE**


This section provides additional information about the ISE to DNAC requirements

- **Passwords:** DNAC uses the ISE CLI password when it connects to ISE to run CLI commands. The CLI and the Admin usernames and passwords must be the same. For details about system passwords, see Administrator Access to Cisco ISE, on page 77.

- **APIs:** DNAC configures some parts of ISE by calling ISE APIs. API access must be enabled in ISE, but do not enable CSRF. For more information, see Enable External RESTful Services APIs, on page 79.

- **pxGrid:** ISE is a pxGrid controller, and DNAC is a subscriber. Both ISE and DNAC monitor the Trustsec topic, which contains SGT and SGACL information. ISE uses a certificate to connect to pxGrid. Clocks must be synchronized between ISE and DNAC in order for the pxGrid connection to work. For more information about pxGrid in ISE, see Enable External RESTful Services APIs, on page 79.

- **ISE IP Address:** The connection between the ISE PAN and DNAC must be direct. It cannot be through a proxy, a load balancer, or virtual IP address. Both ISE and DNAC configure a static address for each other.

  Verify that ISE is not using a proxy. If it is, exclude the DNAC IP from the proxy.

- **SXP:** SXP is not required to communicate with DNAC. You may want to enable SXP when you connect ISE to the DNA-managed network, so ISE can communicate with network devices that don’t have hardware support for Trustsec.

- **Certificate for connections to ISE:**
  - The ISE admin certificate must contain the ISE IP or FQDN in subject name or SAN.
  - ECDSA keys are not supported for SSH keys, ISE SSH access, or in certificates in DNA Center and Cisco ISE.
  - Self-signed certs applied on DNA Center must have the Basic Constraint's extension with cA:TRUE(RFC5280 section-4.2.19).

**TrustSec Dashboard**

The TrustSec dashboard is a centralized monitoring tool for the TrustSec network. The TrustSec dashboard contains the following dashlets:

- **Metrics**
- **Active SGT Sessions**
- **Alarms**
• NAD / SGT Quick View
• TrustSec Sessions / NAD Activity Live Log

**Metrics**

This section displays statistics about the behavior of the TrustSec network. You can select the time frame (for example, past 2 hours, past 2 days, and so on) and the chart type (for example, bars, line, spline).

The latest bar values are displayed on the graphs. It also displays the percentage change from the previous bar. If there is an increase in the bar value, it will be displayed in green with a plus sign. If there is a decrease in the value, it will be displayed in red with a minus sign.

Place your cursor on a bar of a graph to view the time at which the value was calculated and its exact value in the following format: <Value:xxxx Date/Time: xxx>

You can view the following metrics:

<table>
<thead>
<tr>
<th><strong>SGT sessions</strong></th>
<th>Displays the total number of SGT sessions created during the chosen time frame.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong> SGT sessions are the user sessions that received an SGT as part of the authorization flow.</td>
<td></td>
</tr>
<tr>
<td><strong>SGTs in use</strong></td>
<td>Displays the total number of unique SGTs that were used during the chosen time frame. For example, in one hour, if there were 200 TrustSec sessions, but ISE responded with only 6 types of SGTs in the authorization responses, the graph will display a value 6 for this hour.</td>
</tr>
<tr>
<td><strong>Alarms</strong></td>
<td>Displays the total number of alarms and errors that occurred during the chosen time frame. Errors are displayed in red and alarms are displayed in yellow.</td>
</tr>
<tr>
<td><strong>NADs in use</strong></td>
<td>Displays the number of unique NADs, which took part in TrustSec authentications during the chosen time frame.</td>
</tr>
</tbody>
</table>

**Current Network Status**

The middle section of the dashboard displays information about the current status of the TrustSec network. The values displayed in the graphs are updated when the page is loaded and can be refreshed by using the Refresh Dashboard option.

**Active SGT Sessions**

This dashlet displays the SGT sessions that are currently active in the network. You can view the top 10 most used or least used SGTs. The X-axis shows the SGT usage and the Y-axis displays the names of the SGTs.

To view the TrustSec session details for an SGT, click on the bar corresponding to that SGT. The details of the TrustSec sessions related to that SGT are displayed in the Live Log dashlet.

**Alarms**

This dashlet displays the alarms related to the TrustSec sessions. You can view the following details:
• Alarm Severity—Displays an icon that represents the severity level of the alarm.
  • High—Includes the alarms that indicate failure in the TrustSec network (for example, device failed to refresh its PAC). Marked with red icon.
  • Medium—Includes warnings that indicate wrong configuration of the network device (for example, device failed to accept CoA message). Marked with yellow.
  • Low—Includes general information and update on network behavior (for example, configuration changes in TrustSec). Marked with blue.

Quick View

The Quick View dashlet displays TrustSec-related information for NADs. You can also view the TrustSec-related information for an SGT.

NAD Quick View

Enter the name of the TrustSec network device for which you want to view the details in the Search box and press Enter. The search box provides an auto-complete feature, which filters and shows the matched device names in a drop down as the user types into the text box.

The following details are displayed:
  • NDGs—Lists the Network Device Groups (NDGs) to which this network device belongs.
  • IP Address—IP address of the network device. Click on this link to view the NAD activity details in the Live Logs dashlet.
  • Active sessions—Number of active TrustSec sessions connected to this device.
  • PAC expiry—PAC expiry date.
  • Last Policy Refresh—Policy last download date.
  • Last Authentication—Last authentication report timestamp for this device.
  • Active SGTs—Lists the SGTs used in the active sessions that are related to this network device. The number displayed within the brackets denotes the number of sessions that are currently using this SGT. Click on an SGT link to view the TrustSec session details in the Live Log dashlet.

You can use the Show Latest Logs option to view the NAD activity live logs for the device.

SGT Quick View

Enter the name of the SGT for which you want to view the details in the Search box and press Enter.

The following information will be displayed in this dashlet:
  • Value—SGT value (both decimal and hexadecimal).
  • Icon—Displays the icon that is assigned to this SGT.
Live Log

Click the TrustSec Sessions link to view the active TrustSec sessions (sessions that have SGT as part of their response).

Click the NAD Activity link to view information regarding TrustSec protocol data requests and responses from NADs to Cisco ISE.

Configure TrustSec Global Settings

For Cisco ISE to function as an TrustSec server and provide TrustSec services, you must define some global TrustSec settings.

Before you begin

- Before you configure global TrustSec settings, ensure that you have defined global EAP-FAST settings (choose Administration > System > Settings > Protocols > EAP-FAST > EAP-FAST Settings).

  You may change the Authority Identity Info Description to your Cisco ISE server name. This description is a user-friendly string that describes the Cisco ISE server that sends credentials to an endpoint client. The client in a Cisco TrustSec architecture can be either the endpoint running EAP-FAST as its EAP method for IEEE 802.1X authentication or the supplicant network device performing Network Device Access Control (NDAC). The client can discover this string in the protected access credentials (PAC) type-length-value (TLV) information. The default value is Identity Services Engine. You should change the value so that the Cisco ISE PAC information can be uniquely identified on network devices upon NDAC authentication.

- To perform the following task, you must be a Super Admin or System Admin.

Step 1  Choose Work Centers > TrustSec > Settings > General TrustSec Settings.

Step 2  Enter the values in the fields.

Step 3  Click Save.

What to do next

- Configure TrustSec Devices, on page 815
Configure TrustSec Matrix Settings

Before you begin
To perform the following task, you must be a Super Admin or System Admin.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Work Centers &gt; TrustSec &gt; Settings &gt; TrustSec Matrix Settings.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Enter the required details in the TrustSec Matrix Settings page.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Save.</td>
</tr>
</tbody>
</table>

Configure TrustSec Devices
For Cisco ISE to process requests from TrustSec-enabled devices, you must define these TrustSec-enabled devices in Cisco ISE.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Choose Work Centers &gt; TrustSec &gt; Components &gt; Network Devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Add.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the required information in the Network Devices section.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Check the Advanced Trustsec Settings check box to configure a Trustsec-enabled device.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Submit.</td>
</tr>
</tbody>
</table>

OOB TrustSec PAC
All TrustSec network devices possess a TrustSec PAC as part of the EAP-FAST protocol. This is also utilized by the secure RADIUS protocol where the RADIUS shared secret is derived from parameters carried by the PAC. One of these parameters, Initiator-ID, holds the TrustSec network device identity, namely the Device ID.

If a device is identified using TrustSec PAC and there is no match between the Device ID, as configured for that device on Cisco ISE, and the Initiator-ID on the PAC, the authentication fails.

Some TrustSec devices (for example, Cisco firewall ASA) do not support the EAP-FAST protocol. Therefore, Cisco ISE cannot provision these devices with TrustSec PAC over EAP-FAST. Instead, the TrustSec PAC is generated on Cisco ISE and manually copied to the device; hence this is called as the Out of Band (OOB) TrustSec PAC generation.

When you generate a PAC from Cisco ISE, a PAC file encrypted with the Encryption Key is generated.

This section describes the following:

**Related Topics**
- Generate a TrustSec PAC from the Settings Screen, on page 816
- Generate a TrustSec PAC from the Network Devices Screen, on page 816
Generate a TrustSec PAC from the Settings Screen

You can generate a TrustSec PAC from the Settings screen.

**Step 1** Choose Administration > System > Settings.

**Step 2** From the Settings navigation pane on the left, click Protocols.

**Step 3** Choose EAP-FAST > Generate PAC.

**Step 4** Generate TrustSec PAC.

Generate a TrustSec PAC from the Network Devices Screen

You can generate a TrustSec PAC from the Network Devices screen.

**Step 1** Choose Work Centers > TrustSec > Components > Network Devices.

**Step 2** Click Add. You can also click Add new device from the action icon on the Network Devices navigation pane.

**Step 3** If you are adding a new device, provide a device name.

**Step 4** Check the Advanced TrustSec Settings check box to configure a TrustSec device.

**Step 5** Under the Out of Band (OOB) TrustSec PAC sub section, click Generate PAC.

**Step 6** Provide the following details:

- PAC Time to Live—Enter a value in days, weeks, months, or years. By default, the value is one year. The minimum value is one day and the maximum is ten years.

- Encryption Key—Enter an encryption key. The length of the key must be between 8 and 256 characters. The key can contain uppercase or lowercase letters, or numbers, or a combination of alphanumeric characters.

  The Encryption Key is used to encrypt the PAC in the file that is generated. This key is also used to decrypt the PAC file on the devices. Therefore, it is recommended that the administrator saves the Encryption Key for later use.

  The Identity field specifies the Device ID of a TrustSec network device and is given an initiator ID by the EAP-FAST protocol. If the Identity string entered here does not match that Device ID defined under TrustSec section in the Network Device creation page, authentication will fail.

  The expiration date is calculated based on the PAC Time to Live.

**Step 7** Click Generate PAC.

Generate a TrustSec PAC from the Network Devices List Screen

You can generate a TrustSec PAC from the Network Devices list screen.

**Step 1** Choose Work Centers > TrustSec > Components > Network Devices.

**Step 2** Click Network Devices.
Step 3: Check the check box next to a device for which you want to generate the TrustSec PAC and click Generate PAC.

Step 4: Provide the details in the fields.

Step 5: Click Generate PAC.

---

**Push Button**

The Push option in the egress policy initiates a CoA notification that calls the Trustsec devices to immediately request for updates from Cisco ISE regarding the configuration changes in the egress policy.

**Related Topics**

- Update SGT Matrix CoA Flow, on page 845

---

**Configure TrustSec AAA Servers**

You can configure a list of Cisco ISE servers in your deployment in the AAA server list to allow TrustSec devices to be authenticated against any of these servers. When you add Cisco ISE servers to this list, all these server details are downloaded to the TrustSec device. When a TrustSec device tries to authenticate, it chooses any Cisco ISE server from this list and, if the first server is down or busy, the TrustSec device can authenticate itself against any of the other servers from this list. By default, the primary Cisco ISE server is a TrustSec AAA server. We recommend that you configure additional Cisco ISE servers in this AAA server list so that if one server is busy, another server from this list can handle the TrustSec request.

This page lists the Cisco ISE servers in your deployment that you have configured as your TrustSec AAA servers.

You can click the **Push** button to initiate an environment CoA notification after you configure multiple TrustSec AAA servers. This environment CoA notification goes to all TrustSec network devices and provides an update of all TrustSec AAA servers that were changed.

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

---

**Step 1** Choose **Work Centers > TrustSec > Components > TrustSec AAA Servers.**

**Step 2** Click **Add.**

**Step 3** Enter the values as described:

- **Name**—Name that you want to assign to the Cisco ISE server in this AAA Server list. This name can be different from the hostname of the Cisco ISE server.
- **Description**—An optional description.
- **IP**—IP address of the Cisco ISE server that you are adding to the AAA Server list.
- **Port**—Port over which communication between the TrustSec device and server should take place. The default is 1812.
**Step 4**  Click Submit.

---

*What to do next*

Configure Security Groups.

---

**Security Groups Configuration**

A Security Group (SG) or Security Group Tag (SGT) is an element that is used in TrustSec policy configuration. SGTs are attached to packets when they move within a trusted network. These packets are tagged when they enter a trusted network (ingress) and untagged when they leave the trusted network (egress).

SGTs are generated in a sequential manner, but you have the option to reserve a range of SGTs for IP to SGT mapping. Cisco ISE skips the reserved numbers while generating SGTs.

TrustSec service uses these SGTs to enforce the TrustSec policy at egress.

You can configure security groups from the following pages in the Admin portal:

- Work Centers > TrustSec > Components > Security Groups.
- Directly from egress policy page at Configure > Create New Security Group.

You can click the Push button to initiate an environment CoA notification after updating multiple SGTs. This environment CoA notification goes to all TrustSec network devices forcing them to start a policy/data refresh request.

*Related Topics*

- Add Security Groups, on page 818
- Configure SGT from Egress Policy, on page 835
- Configure NDAC Authorization, on page 838
- Configure TrustSec AAA Servers, on page 817

**Add Security Groups**

Each security group in your TrustSec solution should be assigned a unique SGT. Even though Cisco ISE supports 65,535 SGTs, having fewer number of SGTs would enable you to deploy and manage the TrustSec solution easily. We recommend a maximum of 4,000 SGTs.

*Before you begin*

To perform the following task, you must be a Super Admin or System Admin.

---

**Step 1**  Choose Work Centers > TrustSec > Components > Security Groups.

**Step 2**  Click Add to add a new security group.

**Step 3**  Enter a name and description (optional) for the new security group.

**Step 4**  Check the Propagate to ACI check box if you want to propagate this SGT to ACI. The SXP mappings that are related to this SGT will be propagated to ACI only if they belong to a VPN that is selected in the ACI Settings page.
This option is disabled by default.

**Step 5** Enter a Tag Value. Tag value can be set to be entered manually or autogenerate. You can also reserve a range for the SGT. You can configure it from the General TrustSec Settings page (Work Centers > TrustSec > Settings > General TrustSec Settings).

**Step 6** Click Save.

---

**What to do next**

Configure Security Group Access Control Lists

---

**Import Security Groups into Cisco ISE**

You can import security groups into a Cisco ISE node using a comma-separated value (CSV) file. You must first update the template before you can import security groups into Cisco ISE. You cannot run import of the same resource type at the same time. For example, you cannot concurrently import security groups from two different import files.

You can download the CSV template from the Admin portal, enter your security group details in the template, and save the template as a CSV file, which you can then import back into Cisco ISE. While importing security groups, you can stop the import process when Cisco ISE encounters the first error.

**Step 1** Choose Work Centers > TrustSec > Components > Security Groups.
**Step 2** Click Import.
**Step 3** Click Browse to choose the CSV file from the system that is running the client browser.
**Step 4** Check the Stop Import on First Error check box.
**Step 5** Click Import.

---

**Export Security Groups from Cisco ISE**

You can export security groups configured in Cisco ISE in the form of a CSV file that you can use to import these security groups into another Cisco ISE node.

**Step 1** Choose Work Centers > TrustSec > Components > Security Groups.
**Step 2** Click Export.
**Step 3** To export security groups, you can do one of the following:

- Check the check boxes next to the group that you want to export, and choose Export > Export Selected.
- Choose Export > Export All to export all the security groups that are defined.

**Step 4** Save the export.csv file to your local hard disk.
Add IP SGT Static Mapping

You can use the IP-SGT static mappings to deploy the mappings on TrustSec devices and SXP domains in a unified manner. While creating a new IP-SGT static mapping, you can specify the SXP domains and the devices on which you want to deploy this mapping. You can also associate the IP-SGT mapping to a mapping group.

**Step 1** Choose Work Centers > TrustSec > Components > IP SGT Static Mapping.

**Step 2** Click Add.

**Step 3** Enter the hostname or the IP address.

**Step 4** If you want to use an existing mapping group, click Add to a Mapping Group and select the required group from the Mapping Group drop-down list.

If you want to map this IP address/hostname to an SGT individually, click Map to SGT Individually and do the following:

- Select an SGT from the SGT drop-down list.
- Select the SXP VPN groups on which the mapping must be deployed.
- Specify the devices on which you want to deploy this mapping. You can deploy the mapping on all TrustSec devices, on selected network device groups, or on selected network devices.

**Note** After adding the mappings, you must deploy the mappings on the target network devices using the Deploy option. You must do this explicitly even though you have saved the mappings earlier. Click Check Status to check the deployment status of the devices.

**Step 5** Click Save.

Import IP SGT Static Mappings into Cisco ISE

You can import IP SGT mappings using a CSV file.

You can also download the CSV template from the Admin portal, enter your mapping details, save the template as a CSV file, and then import it back into Cisco ISE.

**Step 1** Choose Work Centers > TrustSec > Components > IP SGT Static Mapping.

**Step 2** Click Import.

**Step 3** Click Browse to select the CSV file from the system that is running the client browser.

**Step 4** Click Upload.

Export IP SGT Static Mappings from Cisco ISE

You can export the IP SGT mappings in the form of a CSV file. You can use this file to import these mappings into another Cisco ISE node.
Step 1  Choose Work Centers > TrustSec > Components > IP SGT Static Mapping.
Step 2  Do one of the following:

- Check the check boxes next to the mappings that you want to export, and choose Export > Selected.
- Choose Export > All to export all the mappings.

Step 3  Save the mappings.csv file to your local hard disk.

---

### Add SGT Mapping Group

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

Step 1  Choose Work Centers > TrustSec > Components > IP SGT Static Mapping > Manage Groups.
Step 2  Click Add.
Step 3  Enter a name and description for the mapping group.
Step 4  Do the following:

- Select an SGT from the SGT drop-down list.
- Select the SXP VPN groups on which the mappings must be deployed.
- Specify the devices on which you want to deploy the mappings. You can deploy the mappings on all TrustSec devices, on selected network device groups, or on selected network devices.

Step 5  Click Save.

---

You can move an IP SGT mapping from one mapping group to another mapping group.

You can also update or delete the mappings and mapping groups. To update a mapping or mapping group, check the check box next to the mapping or mapping group that you want to update, and then click Edit. To delete a mapping or mapping group, check the check box next to the mapping or mapping group that you want to delete, and then click Trash > Selected. When a mapping group is deleted, the IP SGT mappings within that group are also deleted.

### Add Security Group Access Control Lists

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

Step 1  Choose Work Centers > TrustSec > Components > Security Group ACLs.
Step 2  Click Add to create a new Security Group ACL.
Step 3

Enter the following information:

- **Name**—Name of the SGACL
- **Description**—An optional description of the SGACL
- **IP Version**—IP version that this SGACL supports:
  - IPv4—Supports IP version 4 (IPv4)
  - IPv6—Supports IP version 6 (IPv6)
  - Agnostic—Supports both IPv4 and IPv6
- **Security Group ACL Content**—Access control list (ACL) commands. For example:

  permit icmp

  deny ip

The syntax of SGACL input is not checked within ISE. Make sure you are using the correct syntax so that switches, routers and access points can apply them without errors. The default policy can be configured as `permit ip, permit ip log, deny ip, or deny ip log`. A TrustSec network device attaches the default policy to the end of the specific cell policy.

Here are two examples of SGACLs for guidance. Both include a final catch all rule. The first one denies as the final catch all rule, and the second one permits.

**Permit_Web_SGACL**

```plaintext
permit tcp dst eq 80
permit tcp dst eq 443
deny ip
```

**Deny_JumpHost_Protoocols**

```plaintext
deny tcp dst eq 23
deny tcp dst eq 23
deny tcp dst eq 3389
permit ip
```

The following table lists syntax for SGACL for IOS, IOS XE and NS-OS operating systems.

<table>
<thead>
<tr>
<th>SGACL CLI and ACEs</th>
<th>Syntax common across IOS, IOS XE, and NX-OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>config acl</td>
<td>deny, exit, no, permit</td>
</tr>
<tr>
<td>deny</td>
<td>ahp, eigrp, gre, icmp, igmp, ip, nos, ospf, pcp, pim, tcp, udp</td>
</tr>
<tr>
<td>permit</td>
<td></td>
</tr>
<tr>
<td>deny tcp</td>
<td>dst, log, src</td>
</tr>
<tr>
<td>deny tcp src</td>
<td></td>
</tr>
<tr>
<td>deny tcp dst</td>
<td></td>
</tr>
<tr>
<td>deny tcp dst eq</td>
<td>&lt;0-65535&gt; port number</td>
</tr>
<tr>
<td>deny tcp src eq</td>
<td></td>
</tr>
<tr>
<td>SGACL CLI and ACEs</td>
<td>Syntax common across IOS, IOS XE, and NX-OS</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>deny udp</td>
<td>Dst, log, src</td>
</tr>
<tr>
<td>deny udp src</td>
<td></td>
</tr>
<tr>
<td>deny udp dest</td>
<td></td>
</tr>
<tr>
<td>deny tcp dst eq www</td>
<td>&lt;0-65535&gt; port number</td>
</tr>
<tr>
<td>deny tcp src eq www</td>
<td></td>
</tr>
</tbody>
</table>

**Step 4**  
Click Submit.

---

**Note**  
Cisco ISE has the following predefined SGACLs: Permit IP, Permit IP Log, Deny IP, and Deny IP Log. You can use these SGACLs to configure the TrustSec Matrix using the GUI or ERS API. Though these SGACLs are not listed in the Security Group ACLs listing page in the GUI, these SGACLs will be listed when you use the ERS API to list the available SGACLs (ERS getAll call).

**Egress Policy**

The egress table lists the source and destination SGTs, both reserved and unreserved. This page also allows you to filter the egress table to view specific policies and also to save these preset filters. When the source SGT tries to reach the destination SGT, the TrustSec-capable device enforces the SGACLs based on the TrustSec policy as defined in the Egress Policy. Cisco ISE creates and provisions the policy.

After you create the SGTs and SGACLs, which are the basic building blocks required to create a TrustSec policy, you can establish a relationship between them by assigning SGACLs to source and destination SGTs.

Each combination of a source SGT to a destination SGT is a cell in the Egress Policy.

You can view the Egress Policy in the **Work Centers > TrustSec > TrustSec Policy > Egress Policy** page.

You can view the Egress policy in three different ways:

- Source Tree View
- Destination Tree View
- Matrix View

**Related Topics**

- [Matrix Operations](#), on page 826
- [Egress Policy Table Cells Configuration](#), on page 833
- [Configure SGT from Egress Policy](#), on page 835
- [The Unknown Security Group](#), on page 836
- [Security Groups Configuration](#), on page 818
- [Security Group Access Control Lists Configuration](#)
Source Tree View

The Source Tree view lists a compact and organized view of source SGTs in a collapsed state. You can expand any source SGT to see the internal table that lists all information related to that selected source SGT. This view displays only the source SGTs that are mapped to destination SGTs. If you expand a specific source SGT, it lists all destination SGTs that are mapped to this source SGT and the corresponding policy (SGACLs) in a table.

You will see three dots (...) next to some fields. This signifies that there is more information contained in the cell. You can position the cursor over the three dots to view the rest of the information in a quick view popup. When you position the cursor over an SGT name or an SGACL name, a quick view popup opens to display the content of that particular SGT or SGACL.

Destination Tree View

The Destination Tree view lists a compact and organized view of destination SGTs in a collapsed state. You can expand any destination SGT to see the internal table that lists all information related to that selected destination SGT. This view displays only the destination SGTs that are mapped to source SGTs. If you expand a specific destination SGT, it lists all source SGTs that are mapped to this destination SGT and the corresponding policy (SGACLs) in a table.

You will see three dots (...) next to some fields. This signifies that there is more information contained in the cell. You can position the cursor over the three dots to view the rest of the information in a quick view popup. When you position the cursor over an SGT name or an SGACL name, a quick view popup opens to display the content of that particular SGT or SGACL.

Matrix View

The Matrix View of the Egress policy looks like a spreadsheet. It contains two axis:

- Source Axis—The vertical axis lists all the source SGTs.
- Destination Axis—The horizontal axis lists all the destination SGTs.

The mapping of a source SGT to a destination SGT is represented as a cell. If a cell contains data, then it represents that there is a mapping between the corresponding source SGT and the destination SGT. There are two types of cells in the matrix view:

- Mapped cells—When a source and destination pair of SGTs is related to a set of ordered SGACLs and has a specified status.
- Unmapped cells—When a source and destination pair of SGTs is not related to any SGACLs and has no specified status.

The Egress Policy cell displays the source SGT, the destination SGT, and the Final Catch All Rule as a single list under SGACLs, separated by commas. The Final Catch All Rule is not displayed if it is set to None. An empty cell in a matrix represents an unmapped cell.

In the Egress Policy matrix view, you can scroll across the matrix to view the required set of cells. The browser does not load the entire matrix data at once. The browser requests the server for the data that falls in the area you are scrolling in. This prevents memory overflow and performance issues.

You can use the following options in the View drop-down list to change the matrix view.
• Condensed with SGACL names—If you select this option, the empty cells are hidden and the SGACL names are displayed in the cells.

• Condensed without SGACL names—The empty cells are hidden and the SGACL names are not displayed in the cells. This view is useful when you want to see more matrix cells and differentiate between the content of the cells using colors, patterns, and icons (cell status).

• Full with SGACL names—If you select this option, the left and upper menus are hidden and the SGACL names are displayed in the cells.

• Full without SGACL names—When this option is selected, the matrix is displayed in full screen mode and the SGACL names are not displayed in the cells.

ISE allows you to create, name, and save the custom views. To create custom views, choose Show > Create Custom View. You can also update the view criteria or delete unused views.

The Matrix view has the same GUI elements as the Source and Destination views. However, it has these additional elements:

**Related Topics**

- [Matrix Operations](#), on page 826

### Matrix Dimensions

The **Dimension** drop-down list in the Matrix view enables you to set the dimensions of the matrix.

### Import/Export Matrix

The **Import** and **Export** buttons enable you to import or export the matrix.

### Create Custom View

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Matrix View page, select the Create Custom View option from the Show drop-down list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Edit View dialog box, enter the following details:</td>
</tr>
<tr>
<td></td>
<td>• View Name—Enter a name for the custom view.</td>
</tr>
<tr>
<td></td>
<td>• Source Security Groups—Move the SGTs that you want to include in the custom view to the Show transfer box.</td>
</tr>
<tr>
<td></td>
<td>• Show Relevant for Destination—Check this check box if you want to override your selection in the Source Security Group Show transfer box and copy all the entries in the Destination Security Group Hide transfer box. If there are more than 200 entries, the data will not be copied and a warning message will be displayed.</td>
</tr>
<tr>
<td></td>
<td>• Destination Security Groups—Move the SGTs that you want to include in the custom view to the Show transfer box.</td>
</tr>
<tr>
<td></td>
<td>• Show Relevant for Source—Check this check box if you want to override your selection in the Destination Security Group Show transfer box and copy all the entries in the Source Security Group Hide transfer box.</td>
</tr>
<tr>
<td></td>
<td>• Sort Matrix By—Select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Manual Order</td>
</tr>
</tbody>
</table>
Matrix Operations

Navigating through the Matrix
You can navigate through the matrix either by dragging the matrix content area with the cursor or by using horizontal and vertical scroll bars. You can click and hold on a cell to drag it along with the entire matrix content in any direction. The source and destination bar moves along with the cells. The matrix view highlights the cell and the corresponding row (Source SGT) and column (Destination SGT) when a cell is selected. The coordinates (Source SGT and Destination SGT) of the selected cell are displayed below the matrix content area.

Selecting a Cell in the Matrix
To select a cell in the matrix view, click on it. The selected cell is displayed in different color, and the source and destination SGTs are highlighted. You can deselect a cell either by clicking it again or by selecting another cell. Multiple cell selection is not allowed in the matrix view. Double-click the cell to edit the cell configuration.

Configure SGACL from Egress Policy
You can create Security Group ACLs directly from the Egress Policy page.

Configure Work Process Settings

Before you begin
To perform the following task, you must be a Super Admin.

Step 1 Choose Work Centers > TrustSec > TrustSec Policy > Egress Policy.
Step 2 From the Source or Destination Tree View page, choose Configure > Create New Security Group ACL.
Step 3 Enter the required details and click Submit.

Step 1 Choose Work Centers > TrustSec > Settings > Work Process Settings.
Step 2 Select one of the following options:

- Single Matrix—Select this option if you want to create only one Policy matrix for all the devices in the TrustSec network.
- Multiple Matrices—Allows you to create multiple policy matrices for different scenarios. You can use these matrices to deploy different policies to different network devices.

Note The matrices are independent and each network device can be assigned to only one matrix.
• Production and Staging Matrices with Approval Process—Select this option if you want to enable the Workflow mode. Select the users that are assigned to the editor and approver roles. You can select the users only from the Policy Admin and Super Admin groups. A user cannot be assigned to both editor and approver roles.

Ensure that email addresses are configured for the users that are assigned to the editor and approver roles, otherwise email notifications regarding the workflow process will not be sent to these users.

When the Workflow mode is enabled, a user that is assigned to the editor role can create a staging matrix, select the devices on which he wants to deploy the staging policy, and submit the staging policy to the approver for approval. The user that is assigned to the approver role can review the staging policy and approve or reject the request. The staging policy can be deployed on the selected network devices only after the staging policy is reviewed and approved by the approver.

Step 3  Check the Use DEFCONS check box if you want to create DEFCON matrices.

DEFCON matrices are standby policy matrices that can be easily deployed in the event of network security breaches. You can create DEFCON matrices for the following severity levels: Critical, Severe, Substantial, and Moderate. When a DEFCON matrix is activated, the corresponding DEFCON policy is immediately deployed on all the TrustSec network devices. You can use the Deactivate option to remove the DEFCON policy from the network devices.

Step 4  Click Save.

Matrices Listing Page

TrustSec policy matrices and DEFCON matrices are listed in the Matrices Listing page (Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrices List). You can also view the number of devices that are assigned to each matrix.

Note
Matrices Listing page is not displayed when Single Matrix mode is enabled with DEFCON matrix option disabled.

You can do the following from the Matrices Listing page:

• Add a new matrix
• Edit an existing matrix
• Delete a matrix
• Duplicate an existing matrix
• Assign NADs to a matrix

You can assign NADs to a matrix by using the Assign NADs option. To do this:

1. In the Assign Network Devices window, select the network devices that you want to assign to a matrix. You can also use the filter option to select the network devices.

2. Select the matrix from the Matrix drop-down list. All the existing matrices and the default matrix are listed in this drop-down list.
After assigning the devices to a matrix, click Push to notify the TrustSec configuration changes to the relevant network devices.

Note the following points while working on the Matrices Listing page:

- You cannot edit, delete, or rename the default matrix.
- While creating a new matrix you can start with a blank matrix or copy the policy from an existing matrix.
- If you delete a matrix, the NADs that are assigned to that matrix are automatically moved to the default matrix.
- When you copy an existing matrix, a copy of the matrix will be created but devices are not automatically assigned to the copied matrix.
- In the Multiple Matrices mode, all the devices are assigned to the default matrix at the initial stage.
- In the Multiple Matrices mode, some of the SGACLs might be shared among the matrices. In such cases, changing an SGACL content will affect all matrices that contain this SGACL in one of their cells.
- Multiple matrices cannot be enabled if staging is in progress.
- When you are moving from Multiple Matrices mode to Single Matrix mode, all the NADs are automatically assigned to the default matrix.
- You cannot delete a DEFCON matrix if it is currently activated.

**TrustSec Matrix Workflow Process**

The Matrix Workflow feature helps you to test a new policy on a limited set of devices by using a draft version of the matrix (called staging matrix) before deploying the policy on all the network devices. You can submit the staging policy for approval and deploy the staging policy on the selected network devices after it is approved. This feature helps you to deploy the new policy on a limited set of devices, check whether it is working fine, and make any changes, if required. You can continue deploying the policy on next set of devices or on all the devices. When the staging policy is deployed on all the network devices, the staging matrix can be set as the new production matrix.

When the Workflow mode is enabled, a user that is assigned to the editor role can create a staging matrix and edit the matrix cells. The staging matrix is a copy of the production matrix that is currently deployed on the TrustSec network. The editor can select the devices on which he wants to deploy the staging policy and submit the staging policy to the approver for approval. The user that is assigned to the approver role can review the staging policy and approve or reject the request. The staging policy can be deployed on the selected network devices only after the staging policy is reviewed and approved by the approver.

The following figure describes the workflow process.
Super Admin user can select the users that are assigned to the editor and approver roles in the Workflow Process Settings page (Work Centers > TrustSec > Settings > Workflow Process).

You cannot edit the SGTs and SGACLs after the staging policy is deployed on the selected devices, however, you can edit the matrix cells. You can use the Configuration Delta report to track the difference between the production matrix and the staging matrix. You can also click on the Delta icon on a cell to view the changes made to that cell during the staging process.

The following table describes the different stages of the workflow:

<table>
<thead>
<tr>
<th>Stage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staging in Edit</td>
<td>The matrix is moved to Staging in Edit state, when an editor starts editing the staging matrix. After editing the staging matrix, the editor can select the devices on which he wants to deploy the new staging policy.</td>
</tr>
<tr>
<td>Stage</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Staging Awaiting Approval</td>
<td>After editing the matrix, the editor submits the staging matrix to the approver for review and approval. While submitting the staging matrix for approval, the editor can add the comments that will be included in the email sent to the approver. The approver can review the staging policy and approve or reject the request. The approver can also view the selected network devices and the Configuration Delta report. While approving or rejecting a request, the approver can add the comments that will be included in the email sent to the editor. The editor can cancel the approval request as long as the staging policy is not deployed on any of the network devices.</td>
</tr>
<tr>
<td>Deploy Approved</td>
<td>When the approver approves the request, the staging matrix is moved to Deploy Approved state. If the request is rejected, the matrix is moved back to Staging in Edit state. The editor can deploy the staging policy on the selected network devices only after the staging policy is approved by the approver.</td>
</tr>
<tr>
<td>Partially Deployed</td>
<td>After the staging matrix is deployed on the selected devices, the matrix is moved to Partially Deployed state. The matrix remains in the Partially Deployed stage till the staging policy is deployed on all the network devices. You cannot edit the SGTs and SGACLs at this stage, however, you can edit the matrix cells. The devices that are not deployed with the latest policy (out-of-sync devices) are displayed in orange (with italic font) in the Network Device Deployment window. This status is also displayed on the deployment progress status bar. The editor can select these devices and request approval to synchronize the devices that were updated in different deployment cycles.</td>
</tr>
<tr>
<td>Fully Deployed</td>
<td>The above process is repeated till the staging policy is deployed on all the network devices. When the staging matrix is deployed on all the network devices, the approver can set the staging matrix as the production matrix. We recommend that you take a copy of the production matrix before setting the staging matrix as the new production matrix, because after replacing the production matrix with the staging matrix, you cannot rollback to the previous version of the production matrix.</td>
</tr>
</tbody>
</table>

The options displayed in the Workflow drop-down list vary based on the workflow state and the user role (editor or approver). The following table lists the menu options displayed for an editor and approver:
<table>
<thead>
<tr>
<th>Workflow state</th>
<th>Menu displayed for Editor</th>
<th>Menu displayed for Approver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Staging in Edit</td>
<td>• Select network devices</td>
<td>• View network devices</td>
</tr>
<tr>
<td></td>
<td>The following options are available in the Network Device Deployment window:</td>
<td>• View deltas</td>
</tr>
<tr>
<td></td>
<td>• Request approval for selected devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Request approval for all/filtered Staging list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Request approval for all/filtered Production list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Request approval for all/filtered devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Request approval for all devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Discard staging</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• View deltas</td>
<td></td>
</tr>
<tr>
<td>Staging Awaiting Approval</td>
<td>• Cancel approval request</td>
<td>• Approve deploy</td>
</tr>
<tr>
<td></td>
<td>• View network devices</td>
<td>• Reject deploy</td>
</tr>
<tr>
<td></td>
<td>The following option is available in the Network Device Deployment window:</td>
<td>• View network devices</td>
</tr>
<tr>
<td></td>
<td>• Cancel approval request</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• View deltas</td>
<td>• Approve deploy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reject deploy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View deltas</td>
</tr>
<tr>
<td>Workflow state</td>
<td>Menu displayed for Editor</td>
<td>Menu displayed for Approver</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>Approved - ready to deploy</td>
<td>• Deploy</td>
<td>• Reject deploy</td>
</tr>
<tr>
<td></td>
<td>• Cancel approval request</td>
<td>• View network devices</td>
</tr>
<tr>
<td></td>
<td>• View network devices</td>
<td>The following option is available in the Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Deployment window:</td>
</tr>
<tr>
<td></td>
<td>• Deploy</td>
<td>• Reject deploy</td>
</tr>
<tr>
<td></td>
<td>• Cancel approval request</td>
<td>• View delta</td>
</tr>
<tr>
<td></td>
<td>• View deltas</td>
<td></td>
</tr>
<tr>
<td>Partially deployed</td>
<td>• Select network devices</td>
<td>• View network devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View delta</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The following options are available in the Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Device Deployment window:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Request approval for selected devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Request approval for all/filtered Staging list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Request approval for all/filtered Production list</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Request approval for all/filtered devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Request approval for all devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• View deltas</td>
</tr>
<tr>
<td>Workflow state</td>
<td>Menu displayed for Editor</td>
<td>Menu displayed for Approver</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------</td>
<td>----------------------------</td>
</tr>
<tr>
<td>Fully deployed</td>
<td>• Select network devices</td>
<td>• Set as production</td>
</tr>
<tr>
<td></td>
<td>The following options are</td>
<td>• View network devices</td>
</tr>
<tr>
<td></td>
<td>available in the Network</td>
<td>• View deltas</td>
</tr>
<tr>
<td></td>
<td>Device Deployment window:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Request approval for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>selected devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Request approval for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>all/filtered Staging list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Request approval for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>all/filtered Production list</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Request approval for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>all/filtered devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Request approval for</td>
<td></td>
</tr>
<tr>
<td></td>
<td>all devices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• View deltas</td>
<td></td>
</tr>
</tbody>
</table>

The workflow options are also available in the Source and Destination Tree view.

You can view the list of devices that downloaded the staging/production policy by using the TrustSec Policy Download report (Work Centers > TrustSec > Reports). The TrustSec Policy Download lists the requests sent by the network devices for policy (SGT/SGACL) download and the details sent by ISE. If the Workflow mode is enabled, the requests can be filtered for production or staging matrix.

**Egress Policy Table Cells Configuration**

Cisco ISE allows you to configure cells using various options that are available in the tool bar. Cisco ISE does not allow a cell configuration if the selected source and destination SGTs are identical to a mapped cell.

**Related Topics**

- Add the Mapping of Egress Policy Cells, on page 833
- Configure SGT from Egress Policy, on page 835

**Add the Mapping of Egress Policy Cells**

You can add the mapping cell for Egress Policy from the Policy page.

**Step 1** Choose **Work Centers > TrustSec > TrustSec Policy > Egress Policy**.

**Step 2** To select the matrix cells, do the following:

- In the matrix view, click a cell to select it.
- In the Source and Destination tree view, check the check box of a row in the internal table to select it.

**Step 3** Click **Add** to add a new mapping cell.
Select appropriate values for:

- Source Security Group
- Destination Security Group
- Status, Security Group ACLs
- Final Catch All Rule

Click Save.

Export Egress Policy

Choose Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrix > Export.

Check the Include Empty Cells check box if you want to include the empty cells (which do not have any SGACL configured) in the exported file.

When this option is enabled, the whole matrix is exported and the empty cells are marked with the "Empty" keyword in the SGACL column.

Note: Ensure that the exported file does not contain more than 500000 lines, otherwise the export may fail.

Select one of the following options:

- Local Disk—Select this option if you want to export the file to a local drive.
- Repository—Select this option if you want to export the file to a remote repository.

You must configure the repositories before exporting the file. To configure the repositories, choose Administration > Maintenance > Repository. Ensure that read and write access privileges are provided for the repository that you have selected.

You can encrypt the exported file by using an encryption key.

You can modify the file name. File name should not include more than 50 characters. By default, the file name includes the current time, however, if the same file name exists on the remote repository, the file will be overwritten.

Click Export.

Import Egress Policy

You can create the egress policy offline and then import it in to Cisco ISE. If you have a large number of security group tags, then creating the security group ACL mapping one by one might take some time. Instead, creating the egress policy offline and importing it in to Cisco ISE saves time for you. During import, Cisco ISE appends the entries from the CSV file to the egress policy matrix and does not overwrite the data.

Egress policy import fails if the:

- Source or destination SGTs do not exist
- SGACL does not exist
• Monitor status is different than what is currently configured in Cisco ISE for that cell

---

**Step 1** Choose Work Centers > TrustSec > TrustSec Policy > Egress Policy > Matrix > Import.

**Step 2** Click Generate a Template.

**Step 3** Download the template (CSV file) from the Egress Policy page and enter the following information in the CSV file:

  • Source SGT
  • Destination SGT
  • SGACL
  • Monitor status (enabled, disabled, or monitored)

**Step 4** Check the Overwrite Existing Data with New Data check box if you want to overwrite the existing policy with the one that you are importing. If empty cells (cells that are marked with the "Empty" keyword in the SGACL column) are included in the imported file, the existing policy in the corresponding matrix cells will be deleted.

While exporting the egress policy, if you want to include the empty cells, check the Include Empty Cells check box. For more information, see Export Egress Policy, on page 834.

**Step 5** Click Validate File to validate the imported file. Cisco ISE validates the CSV structure, SGT names, SGACL, and file size before importing the file.

**Step 6** Check the Stop Import on First Error check box for Cisco ISE to abort the import if it encounters any errors.

**Step 7** Click Import.

---

**Configure SGT from Egress Policy**

You can create Security Groups directly from the Egress Policy page.

**Step 1** Choose Work Centers > TrustSec > TrustSec Policy > Egress Policy.

**Step 2** From the Source or Destination Tree View page, choose Configure > Create New Security Group.

**Step 3** Enter the required details and click Submit.

---

**Monitor Mode**

The Monitor All option in the egress policy allows you to change the entire egress policy configuration status to monitor mode with a single click. Check the Monitor All check box in the egress policy page to change the egress policy configuration status of all the cells to monitor mode. When you check the Monitor All check box, the following changes take place in the configuration status:

  • The cells whose status is Enabled will act as monitored but appears as if they are enabled.
  • The cells whose status is Disable will not be affected.
  • The cells whose status is Monitor will remain Monitored.
Uncheck the Monitor All check box to restore the original configuration status. It does not change the actual status of the cell in the database. When you deselect Monitor All, each cell in the egress policy regains its original configuration status.

Features of Monitor Mode

The monitoring functionality of the monitor mode helps you to:

• Know how much traffic is filtered but monitored by the monitor mode
• Know that SGT-DGT pair is in monitor mode or enforce mode, and observe if there is any unusual packet drop is happening in the network
• Understand that SGACL drop is actually enforced by enforce mode or permitted by monitor mode
• Create custom reports based on the type of mode (monitor, enforce, or both)
• Identify which SGACL has been applied on NAD and display discrepancy, if any

Related Topics

Run Top N RBACL Drops by User Report, on page 852

The Unknown Security Group

The Unknown security group is a pre-configured security group that cannot be modified and represents the Trustsec with tag value 0.

The Cisco security group network devices request for cells that refer to the unknown SGT when they do not have an SGT of either source or destination. If only the source is unknown, the request applies to the <unknown, Destination SGT> cell. If only the destination is unknown, the request applies to the <source SGT, unknown> cell. If both the source and destination are unknown, the request applies to the <Unknown, Unknown> cell.

Default Policy

Default Policy refers to the <ANY,ANY> cell. Any source SGT is mapped to any destination SGT. Here, the ANY SGT cannot be modified and it is not listed in any source or destination SGTs. The ANY SGT can only be paired with ANY SGT. It cannot be paired with any other SGTs. A TrustSec network device attaches the default policy to the end of the specific cell policy.

• If a cell is empty, that means it contains the default policy alone.

• If a cell contains some policy, the resulting policy is a combination of the cell specific policy followed by the default policy.

According to Cisco ISE, the cell policy and the default policy are two separate sets of SGACLs that the devices get in response to two separate policy queries.

Configuration of the default policy is different from other cells:

• Status can take only two values, Enabled or Monitored.

• Security Group ACLs is an optional field for the default policy, so can be left empty.

• Final Catch All Rule can be any of the following: Permit IP, Deny IP, Permit IP log, or Deny IP log. Clearly the None option is not available here because there is no safety net beyond the default policy.
Push Button

The Push option in the egress policy initiates a CoA notification that calls the Trustsec devices to immediately request for updates from Cisco ISE regarding the configuration changes in the egress policy.

Related Topics

Update SGT Matrix CoA Flow, on page 845

SGT Assignment

Cisco ISE allows you to assign an SGT to a TrustSec device if you know the device hostname or IP address. When a device with the specific hostname or IP address joins the network, Cisco ISE will assign the SGT before authenticating it.

The following SGTs are created by default:

- SGT_TrustSecDevices
- SGT_NetworkServices
- SGT_Employee
- SGT_Contractor
- SGT_Guest
- SGT_ProductionUser
- SGT_Developer
- SGT_Auditor
- SGT_PointofSale
- SGT_ProductionServers
- SGT_DevelopmentServers
- SGT_TestServers
- SGT_PCIServers
- SGT_BYOD
- SGT_Quarantine

Sometimes, devices need to be manually configured to map the security group tags to the endpoint. You can create this mapping from the Security Group Mappings page. Before you perform this action, ensure that you have reserved a range of SGTs.

ISE allows you to create up to 10,000 IP-to-SGT mappings. You can create IP-to-SGT mapping groups to logically group such large scale mappings. Each group of IP-to-SGT mappings contains a list of IP addresses, a single security group it would map to and a network device or network device group which is the deployment target for those mappings.
NDAC Authorization

You can configure the TrustSec policy by assigning SGTs to devices. You can assign security groups to devices based on TrustSec device ID attribute.

Related Topics
- Configure TrustSec Global Settings, on page 814
- Configure TrustSec AAA Servers, on page 817

Configure NDAC Authorization

Before you begin
- Ensure that you create the security groups for use in the policy.
- To perform the following task, you must be a Super Admin or System Admin.

---

Step 1  Choose **Work Centers** > **TrustSec** > **TrustSec Policy** > **Network Device Authorization**.
Step 2  Click the **Action** icon on the right-hand side of the Default Rule row, and click **Insert New Row Above**.
Step 3  Enter the name for this rule.
Step 4  Click the plus sign (+) next to **Conditions** to add a policy condition.
Step 5  You can click **Create New Condition (Advance Option)** and create a new condition.
Step 6  From the **Security Group** drop-down list, select the SGT that you want to assign if this condition evaluates to true.
Step 7  Click the **Action** icon from this row to add additional rules based on device attributes either above or below the current rule. You can repeat this process to create all the rules that you need for the TrustSec policy. You can drag and drop the rules to reorder them by clicking the icon. You can also duplicate an existing condition, but ensure that you change the policy name.

The first rule that evaluates to true determines the result of the evaluation. If none of the rules match, the default rule will be applied; you can edit the default rule to specify the SGT that must be applied to the device if none of the rules match.

Step 8  Click **Save** to save your TrustSec policy.

If a TrustSec device tries to authenticate after you have configured the network device policy, the device will get its SGT and the SGT of its peers and will be able to download all the relevant details.

---

Configure End User Authorization

Cisco ISE allows you to assign a security group as the result of an authorization policy evaluation. Using this option, you can assign a security group to users and end points.

Before you begin
- Read the information on authorization policies.
- To perform the following task, you must be a Super Admin or System Admin.
Step 1  Choose Work Centers > TrustSec > Authorization Policy.
Step 2  Create a new authorization policy.
Step 3  Select a security group, for Permissions.

If the conditions specified in this authorization policy is true for a user or endpoint, then this security group will be assigned to that user or endpoint and all data packets that are sent by this user or endpoint will be tagged with this particular SGT.

TrustSec Configuration and Policy Push

Cisco ISE supports Change of Authorization (CoA) which allows Cisco ISE to notify TrustSec devices about TrustSec configuration and policy changes, so that the devices can reply with requests to get the relevant data. A CoA notification can trigger a TrustSec network device to send either an Environment CoA or a Policy CoA.

You can also push a configuration change to devices that do not intrinsically support the TrustSec CoA feature.

Related Topics
- CoA Supported Network Devices, on page 839
- Environment CoA Notification Flow, on page 841
- Update SGACL Content Flow, on page 843
- Policies Update CoA Notification Flow, on page 845
- Update SGT Matrix CoA Flow, on page 845
- TrustSec CoA Summary, on page 846

CoA Supported Network Devices

Cisco ISE sends CoA notifications to the following network devices:

- Network device with single IP address (subnets are not supported)
- Network device configured as a TrustSec device
- Network device set as CoA supported

When Cisco ISE is deployed in a distributed environment where there are several secondaries that interoperate with different sets of devices, CoA requests are sent from Cisco ISE primary node to all the network devices. Therefore, TrustSec network devices need to be configured with the Cisco ISE primary node as the CoA client.

The devices return CoA NAK or ACK back to the Cisco ISE primary node. However, the following TrustSec session coming from the network device would be sent to the Cisco ISE node to which the network device sends all it's other AAA requests and not necessarily to the primary node.
**Push Configuration Changes to Non-CoA Supporting Devices**

Some platforms do not support Cisco ISE's "Push" feature for Change of Authorization (CoA), for example: some versions of the Nexus network device. For this case, ISE will connect to the network device and make it to trigger an updated configuration request towards ISE. To achieve this, ISE opens an SSHv2 tunnel to the network device, and the Cisco ISE sends a command that triggers a refresh of the TrustSec policy matrix. This method can also be carried on network platforms that support CoA pushing.

### Step 1
Choose **Work Centers** > **Device Administration** > **Network Resources** > **Network Devices**.

### Step 2
Check the checkbox next to the required network device and click **Edit**.
Verify that the network device's name, IP address, RADIUS and TrustSec settings are properly configured.

### Step 3
Scroll down to **Advanced TrustSec Settings**, and in the **TrustSec Notifications and Updates** section, check the **Send configuration changes to device** checkbox, and click the **CLI (SSH)** radio button.

### Step 4
(Optional) Provide an SSH key.

### Step 5
Check the **Include this device when deploying Security Group Tag Mapping Updates** check box, for this SGA device to obtain the IP-SGT mappings using device interface credentials.

### Step 6
Enter the username and password of the user having privileges to edit the device configuration in the Exec mode.

### Step 7
(Optional) Enter the password to enable Exec mode password for the device that would allow you to edit its configuration. You can click **Show** to display the Exec mode password that is already configured for this device.

### Step 8
Click **Submit** at the bottom of the page.

The network device is now configured to push Trustsec changes. After you change a Cisco ISE policy, click **Push** to have the new configuration reflected on the network device.

### SSH Key Validation

You may want to harden security by using an SSH key. Cisco ISE supports this with its SSH key validation feature.

To use this feature, you open an SSHv2 tunnel from the Cisco ISE to the network device, then use the network device's own CLI to retrieve the SSH key. You then copy this key and paste it into Cisco ISE for validation. Cisco ISE terminates the connection if the SSH key is wrong.

**Limitation**: Currently, Cisco ISE can validate only one IP (not on ranges of IP, or subnets within an IP)

**Before you begin**

You will require:

- Login credentials
- CLI command to retrieve the SSH key

for the network device with which you want the Cisco ISE to communicate securely.

### Step 1
On the network device:

a) Log on to the network device with which you want the Cisco ISE to communicate using SSH key validation.
b) Use the device's CLI to show the SSH key.

   **Example:**
   
   For Catalyst devices, the command is: `sho ip ssh`.

c) Copy the SSH key which is displayed.

**Step 2**  
From the Cisco ISE user interface:

a) Choose **Work Centers** > **Device Administration** > **Network Resources** > **Network Devices**, and verify the required network device's name, IP address, RADIUS and TrustSec settings are properly configured.

b) Scroll down to **Advanced TrustSec Settings**, and in the **TrustSec Notifications and Updates** section, check the **Send configuration changes to device** checkbox, and click the **CLI (SSH)** radio button.

c) In the **SSH Key** field, paste the SSH key retrieved previously from the network device.

d) Click **Submit** at the bottom of the page.

The network device is now communicating with the Cisco ISE using SSH key validation.

**Environment CoA Notification Flow**

The following figure depicts the Environment CoA notification flow.

*Figure 59: Environment CoA Notification Flow*

1. Cisco ISE sends an environment CoA notification to the TrustSec network device.

2. The device returns an environment data request.
3. In response to the environment data request, Cisco ISE returns:
   The environment data of the device that sent the request—This includes the TrustSec device’s SGT (as inferred from the NDAC policy) and download environment TTL.
   The name and generation ID of the TrustSec AAA server list.
   The names and generation IDs of (potentially multiple) SGT tables—These tables list SGT name versus SGT value, and together these tables hold the full list of SGTs.

4. If the device does not hold a TrustSec AAA server list, or the generation ID is different from the generation ID that is received, the device sends another request to get the AAA server list content.

5. If the device does not hold an SGT table listed in the response, or the generation ID is different from the generation ID that is received, the device sends another request to get the content of that SGT table.

Environment CoA Triggers

An Environment CoA can be triggered for:

- Network devices
- Security groups
- AAA servers

Related Topics

- Trigger Environment CoA for Network Devices, on page 842
- Trigger Environment CoA for Security Groups, on page 842
- Trigger Environment CoA for TrustSec AAA Servers, on page 843

Trigger Environment CoA for Network Devices

To trigger an Environment CoA for the Network devices, complete the following steps:

---

Step 1 Choose Work Centers > Device Administration > Network Resources > Network Devices.
Step 2 Add or edit a network device.
Step 3 Update TrustSec Notifications and Updates parameters under the Advanced TrustSec Settings section.

Changing the environment attribute is notified only to the specific TrustSec network device where the change took place. Because only a single device is impacted, an environmental CoA notification is sent immediately upon submission. The result is a device update of its environment attribute.

---

Trigger Environment CoA for Security Groups

To trigger an Environment CoA for the security groups, complete the following steps:

---

Step 1 Choose Work Centers > TrustSec > Components > Security Groups.
Step 2 In the Security Group page, change the name of an SGT, which will change the name of the mapping value of that SGT. This triggers an environmental change.
Step 3  Click the **Push** button to initiate an environment CoA notification after changing the names of multiple SGTs. This environment CoA notification goes to all TrustSec network devices and provides an update of all SGTs that were changed.

**Trigger Environment CoA for TrustSec AAA Servers**

To trigger an Environment CoA for the TrustSec AAA servers, complete the following steps.

**Step 1**  Choose **Work Centers > TrustSec > Components > TrustSec AAA Servers**.

**Step 2**  In the TrustSec AAA Servers page create, delete or update the configuration of a TrustSec AAA server. This triggers an environment change.

**Step 3**  Click the **Push** button to initiate an environment CoA notification after you configure multiple TrustSec AAA servers. This environment CoA notification goes to all TrustSec network devices and provides an update of all TrustSec AAA servers that were changed.

**Trigger Environment CoA for NDAC Policy**

To trigger an Environment CoA for the NDAC Policies, complete the following steps.

**Step 1**  Choose **Work Centers > TrustSec > Policy > Network Device Authorization**.

In the NDAC policy page you can create, delete, or update rules of the NDAC policy. These environment changes are notified to all network devices.

**Step 2**  Choose **Work Centers > TrustSec > TrustSec Policy > Network Device Authorization**.

In the NDAC policy page you can create, delete, or update rules of the NDAC policy. These environment changes are notified to all network devices.

**Step 3**  You can initiate an environment CoA notification by clicking the **Push** button in the NDAC policy page. This environment CoA notification goes to all TrustSec network devices and provides an update of network device own SGT.

**Update SGACL Content Flow**

The following figure depicts the Update SGACL Content flow.
1. Cisco ISE sends an update SGACL named list CoA notification to a TrustSec network device. The notification contains the SGACL name and the generation ID.

2. The device may replay with an SGACL data request if both of the following terms are fulfilled:
   - If the SGACL is part of an egress cell that the device holds. The device holds a subset of the egress policy data, which are the cells related to the SGTs of its neighboring devices and endpoints (egress policy columns of selected destination SGTs).
   - The generation ID in the CoA notification is different from the generation ID that the device holds for this SGACL.

3. In response to the SGACL data request, Cisco ISE returns the content of the SGACL (the ACE).

**Initiate an Update SGACL Named List CoA**

To trigger an Update SGACL Named List CoA, complete the following steps:

**Step 1** Choose **Work Centers > TrustSec > Components > Security Group ACLs**.

**Step 2** Change the content of the SGACL. After you submit a SGACL, it promotes the generation ID of the SGACL.

**Step 3** Click the **Push** button to initiate an Update SGACL Named List CoA notification after you change the content of multiple SGACLs. This notification goes to all TrustSec network devices, and provides an update of that SGACL content on the relevant devices.

Changing the name or the IP version of an SGACL does not change its generation ID; hence it does not require sending an update SGACL named list CoA notification.

However, changing the name or IP version of an SGACL that is in use in the egress policy indicates a change in the cell that contains that SGACL, and this changes the generation ID of the destination SGT of that cell.
Policies Update CoA Notification Flow

The following figure depicts the Policies CoA Notification flow.

1. Cisco ISE sends an update policies CoA notification to a TrustSec network device. The notification may contain multiple SGACL names and their generation IDs, and multiple SGT values and their generation IDs.
2. The device may replay with multiple SGACL data requests and/or multiple SGT data.
3. In response to each SGACL data request or SGT data request, Cisco ISE returns the relevant data.

Update SGT Matrix CoA Flow

The following figure depicts the Update SGT Matrix CoA flow.
1. Cisco ISE sends an updated SGT matrix CoA notification to a TrustSec network device. The notification contains the SGT value and the generation ID.

2. The device may replay with an SGT data request if both the following terms are fulfilled:
   - If the SGT is the SGT of a neighboring device or endpoint, the device downloads and hold the cells related to SGTs of neighboring devices and endpoints (a destination SGT).
   - The generation ID in the CoA notification is different from the generation ID that the device holds for this SGT.

3. In response to the SGT data request, Cisco ISE returns the data of all egress cells, such as the source and destination SGTs, the status of the cell, and an ordered list of the SGACL names configured in that cell.

### Initiate Update SGT Matrix CoA from Egress Policy

**Step 1**  
Choose WorkCenters > TrustSec > TrustSec Policy > Egress Policy.

**Step 2**  
On the Egress Policy page, change the content of a cell (status, SGACLs).

**Step 3**  
After you submit the changes, it promotes the generation ID of the destination SGT of that cell.

**Step 4**  
Click the Push button to initiate the Update SGT matrix CoA notification after you change the content of multiple egress cells. This notification goes to all TrustSec network devices, and provides an update of cells content on the relevant devices.

### TrustSec CoA Summary

The following table summarizes the various scenarios that may require initiating a TrustSec CoA, the type of CoA used in each scenario, and the related UI pages.

<table>
<thead>
<tr>
<th>UI Page</th>
<th>Operation that triggers CoA</th>
<th>How it is triggered</th>
<th>CoA type</th>
<th>Send to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Device</td>
<td>Changing the environment TTL in the TrustSec section of the page</td>
<td>Upon successful Submit of TrustSec network device</td>
<td>Environment</td>
<td>The specific network device</td>
</tr>
<tr>
<td>TrustSec AAA Server</td>
<td>Any change in the TrustSec AAA server (create, update, delete, reorder)</td>
<td>Accumulative changes can be pushed by clicking the Push button on the TrustSec AAA servers list page.</td>
<td>Environment</td>
<td>All TrustSec network devices</td>
</tr>
</tbody>
</table>
Security Group Tag Exchange Protocol

Security Group Tag (SGT) Exchange Protocol (SXP) is used to propagate the SGTs across network devices that do not have hardware support for TrustSec. SXP is used to transport an endpoint's SGT along with the IP address from one SGT-aware network device to another. The data that SXP transports is called as IP-SGT mapping. The SGT to which an endpoint belongs can be assigned statically or dynamically, and the SGT can be used as a classifier in network policies.

SXP uses TCP as its transport protocol to set up SXP connection between two separate network devices. Each SXP connection has one peer designated as SXP speaker and the other peer as SXP listener. The peers can also be configured in a bi-directional mode where each of them act as both speaker and listener. Connections can be initiated by either peers, but mapping information is always propagated from a speaker to a listener.
Session bindings are always propagated on the default SXP domain.

The following table lists some of the common terms used in the SXP environment:

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP-SGT mapping</td>
<td>The IP Address to SGT mapping that is exchanged over SXP connection.</td>
</tr>
<tr>
<td></td>
<td>To view all the mappings learned by the SXP devices (including static mappings and session mappings), choose Work Centers &gt; TrustSec &gt; SXP &gt; All SXP Mappings.</td>
</tr>
<tr>
<td>SXP Speaker</td>
<td>The peer that sends the IP-SGT mappings over the SXP connection.</td>
</tr>
<tr>
<td>SXP Listener</td>
<td>The peer that receives the IP-SGT mappings over the SXP connection.</td>
</tr>
</tbody>
</table>

To view the SXP peer devices that are added to Cisco ISE, choose Work centers > TrustSec > SXP > SXP Devices.

We recommend that you run the SXP service on a standalone node.

Note the following points while using the SXP service:

- Cisco ISE does not support multiple SXP session bindings with same IP address.
- If the RADIUS accounting updates are too frequent (for example, around 6 to 8 accounting updates in few seconds), sometimes the accounting update packet might be dropped and SXP might not receive the IP-SGT binding.
- After upgrading from a previous version of ISE, SXP does not start automatically. After the upgrade, you must change the SXP password and restart the SXP process.

### Add an SXP Device

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

1. **Step 1** Choose Work Centers > TrustSec > SXP > SXP Devices.
2. **Step 2** Click Add.
3. **Step 3** Enter the device details:
   - Click Upload from a CSV file to add the SXP devices using a CSV file. Browse and select the CSV file, and then click Upload.

You can also download the CSV template file, fill in the details of the devices that you want to add, and upload the CSV file.
• Click **Add Single Device** to add the device details manually for each SXP device.

Enter the name, IP address, SXP role (listener, speaker, or both), password type, SXP version, and connected PSNs for the peer device. You must also specify the SXP domain to which the peer device is connected.

**Step 4**  
(Optional) Click **Advanced Settings** and enter the following details:

• **Minimum Acceptable Hold Timer**—Specify the time, in seconds, a speaker will send keepalive messages for keeping the connection alive. The valid range is from 1 to 65534.

• **Keep Alive Timer**—Used by a speaker to trigger the dispatch of keepalive messages during intervals when no other information is exported via update messages. The valid range is from 0 to 64000.

**Step 5**  
Click **Save**.

---

**Add an SXP Domain Filter**

You can view all the mappings learned by the SXP devices (including static mappings and session mappings) on the **Work Centers > TrustSec > SXP > All SXP Mappings** page.

By default, session mappings learnt from the network devices are sent only to the default VPN group. You can create SXP domain filters to send the mappings to different SXP domains (VPNs).

To add an SXP domain filter:

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

**Step 1**  
Choose **Work Centers > TrustSec > SXP > All SXP Mappings**.

**Step 2**  
Click **Add SXP Domain Filter**.

**Step 3**  
Do the following:

• Enter the subnet details. The session mappings of the network devices with IP addresses from this subnet are sent to the SXP domain (VPN) that is selected in the **SXP Domain** field.

• Select an SGT from the SGT drop-down list. The session mappings that are related to this SGT are sent to the SXP domain that is selected in the **SXP Domain** field.

If you have specified both Subnet and SGT, the session mappings that match this filter are sent to the SXP domain that you have selected in the **SXP Domain** field.

• Select the SXP domain to which the mappings must be sent.

**Step 4**  
Click **Save**.

---

You can also update or delete the SXP domain filters. To update a filter, click **Manage SXP Domain Filter**, check the check box next to the filter that you want to update, and then click **Edit**. To delete a filter, check the check box next to the filter that you want to delete, and then click **Trash > Selected**.
Configure SXP Settings

Before you begin

To perform the following task, you must be a Super Admin or System Admin.

Step 1  Choose Work Centers > TrustSec > Settings > SXP Settings.

Step 2  Enter the required details in the SXP Settings page.

If you uncheck the Publish SXP Bindings on PxGrid check box, the IP-SGT mappings will not be propagated across the network devices.

Step 3  Click Save.

Note  When the SXP settings are changed, the SXP service is restarted.

TrustSec-ACI Integration

Cisco ISE allows you to synchronize SGTs and SXP mappings with the Internal Endpoint Groups (IEPGs), External Endpoint Groups (EEPGs), and endpoint (EP) configuration of Cisco Application Centric Infrastructure (ACI).

Cisco ISE supports packets coming from the ACI domain to the TrustSec domain by synchronizing the IEPGs and creating correlating read-only SGTs in ISE. These SGTs are used to map the endpoints configured in ACI and create correlating SXP mappings in ISE. These SGTs are displayed on the Security Groups page (with the value "ACI" in the Learned From field). You can view the SXP mappings on the All SXP Mappings page. These mappings are propagated to ACI only if the Policy Plane option is selected (in the ACI Settings page) and the SXP device belongs to an SXP domain that is selected in the ACI Settings page.

Note  The read-only SGTs cannot be used in IP-SGT mappings, mapping groups, and SXP local mappings.

You can select the SGTs that are propagated to ACI. While adding a Security Group, you can specify whether the SGT should be propagated to ACI or not by using the Propagate to ACI option. When this option is enabled, the SXP mappings that are related to this SGT are propagated to ACI if the Policy Plane option is selected (in the ACI Settings page) and the SXP device belongs to a VPN that is selected in the ACI Settings page.

ACI supports the packets coming from the TrustSec domain to the ACI domain by synchronizing the SGTs and creating correlating EEPGs. ACI creates subnets under EEPG based on the SXP mappings that are propagated from Cisco ISE. These subnets are not deleted from ACI, when the corresponding SXP mappings are deleted in Cisco ISE.

When an IEPG is updated in ACI, the corresponding SGT configuration is updated in Cisco ISE. A new EEPG is created in ACI, when an SGT is added in Cisco ISE. When an SGT is deleted, the corresponding EEPG will be deleted in ACI. When an endpoint is updated in ACI, the corresponding SXP mapping is updated in Cisco ISE.
If the connection with the ACI server is lost, Cisco ISE re-synchronizes the data again when the connection is reestablished.

---

**Note**

You must enable the SXP service to use the ACI integration feature.

---

## Configure ACI Settings

### Before you begin

To perform the following task, you must be a Super Admin or System Admin.

### Step 1

Import the ACI certificate into the Trusted Certificates Store. Choose **Administration > System > Certificates > Trusted Certificates > Import** to import the certificate.

### Step 2

Choose **Work Centers > TrustSec > Settings > ACI Settings**.

### Step 3

Check the **TrustSec-ACI Policy Element Exchange** check box to synchronize SGTs and SXP mappings with IEPGs, EEPGs, and endpoint configuration of ACI.

### Step 4

Select one of the following options:

- **Policy Plane**—Select this option if you want Cisco ISE to interact only with APIC data center to interchange SGT, EPG, and SXP information.

- **Data Plane**—If you select this option, in addition to SGT and EPG, additional information is provided to the ASR devices that are connected between the TrustSec network and the APIC-controlled network. These ASR devices must contain the Translation tables for SGT-to-EPG and EPG-to-SGT conversion.

  **Note**

  SXP mappings are not propagated to ACI if you select the Data Plane option.

### Step 5

Enter the following details if you have selected the Policy Plane option:

- **IP address/Hostname**—Enter the IP address or hostname of the ACI server. You can enter three IP addresses or host names separated by commas.

- **Admin Name/Password**—Enter the username and password of the ACI admin user.

- **Tenant**—Enter the name of the tenant that is configured on the ACI.

- **L3 Route Network Name**—Enter the name of the Layer 3 Route network that is configured on the ACI for synchronizing the policy elements.

  Click **Test Settings** to check the connectivity with the ACI server.

- **New SGT Suffix**—This suffix will be added to the SGTs that are newly created based on the EPGs learnt from ACI.

  **Note**

  The EPG name will be truncated if it is greater than 32 characters. However, you can view the full name of the EPG, application profile name, and SGT suffix details in the Description field in the Security Groups listing page.

- **New EPG Suffix**—This suffix will be added to the EPGs that are newly created in ACI based on the SGTs learnt from Cisco ISE.
In the SXP Propagation area, you can select all the SXP domains or specify the SXP domains that will share the mappings with ACI.

### Step 6
Enter the following details if you have selected the Data Plane option:

- **Propagate using SXP**—Check this check box if you want Cisco ISE to learn Endpoint (EP) data from ACI and propagate the EP data using SXP.

  * **Note**: When you select this option, ensure that the SXP service is enabled on the deployment node (Administration > System > Deployment).

- **IP address/Hostname**—Enter the IP address or hostname of the ACI server. You can enter three IP addresses or host names separated by commas.
- **Admin Name/Password**—Enter the username and password of the ACI admin user.
- **Tenant**—Enter the name of the tenant that is configured on the ACI.

  Click **Test Settings** to check the connectivity with the ACI server.

- **Max number of IEPGs**—Specify the maximum number of IEPGs that will be converted to SGTs. IEPGs are converted in alphabetical order. Default value is 1000.
- **Max number of SGTs**—Specify the maximum number of SGTs that will be converted to IEPGs. SGTs are converted in alphabetical order. Default value is 500.
- **New SGT Suffix**—This suffix will be added to the SGTs that are newly created based on the EPGs learnt from ACI.
- **New EPG Suffix**—This suffix will be added to the EPGs that are newly created in ACI based on the SGTs learnt from Cisco ISE.
- **EEPG name for untagged packets**—TrustSec packets that are not converted to an EEPG are tagged with this name in ACI.

### Step 7
Click **Save**.

---

### Run Top N RBACL Drops by User Report
You can run the Top N RBACL Drops by User report to see the policy violations (based on packet drops) by specific users.

**Step 1** Choose **Operations > Reports > TrustSec**.

**Step 2** Click **Top N RBACL Drops by User**.

**Step 3** From the **Filters** drop-down menu, add the required monitor modes.

**Step 4** Enter the values for the selected parameters accordingly. You can specify the mode from the Enforcement mode drop-down list as Enforce, Monitor, or Both.

**Step 5** From the **Time Range** drop-down menu, choose a time period over which the report data will be collected.

**Step 6** Click **Run** to run the report for a specific period, along with the selected parameters.
PART VI

Monitoring and Troubleshooting Cisco ISE

• Monitoring and Troubleshooting, on page 855
• Reports, on page 905
CHAPTER 28

Monitoring and Troubleshooting

• Monitoring and Troubleshooting Service in Cisco ISE, on page 855
• Device Configuration for Monitoring, on page 859
• Troubleshooting the Anyconnect Agent Download Issues, on page 859
• Troubleshooting the Profiler Feed, on page 859
• Posture Compliance, on page 860
• SNMP Traps To Monitor Cisco ISE Processes, on page 860
• Cisco ISE Alarms, on page 862
• Log Collection, on page 880
• Live Authentications, on page 881
• Global Search for Endpoints, on page 882
• Session Trace for an Endpoint, on page 884
• Authentication Summary Report, on page 886
• Diagnostic Troubleshooting Tools, on page 887
• Session Trace Test Cases, on page 889
• Technical Support Tunnel for Advanced Troubleshooting, on page 890
• TCP Dump Utility to Validate the Incoming Traffic, on page 892
• Download Endpoint Statistical Data From Monitoring Nodes, on page 895
• Obtaining Additional Troubleshooting Information, on page 896
• Monitoring Database, on page 901
• Database Crash/File Corruption Issues, on page 903

Monitoring and Troubleshooting Service in Cisco ISE

The Monitoring and troubleshooting service is a comprehensive identity solution for all Cisco ISE run-time services. The Operations menu contains the following components and can be viewed only from the Primary PAN. The Operations menu does not appear in the primary Monitoring node.

• Monitoring—Provides a real-time presentation of meaningful data representing the state of access activities on a network. This insight allows you to easily interpret and affect operational conditions.

• Troubleshooting—Provides contextual guidance for resolving access issues on networks. You can then address user concerns and provide a resolution in a timely manner.

• Reporting—Provides a catalog of standard reports that you can use to analyze trends and monitor system performance and network activities. You can customize reports in various ways and save them for future
use. You can search records using wild cards and multiple values in all reports for the following fields—Identity, Endpoint ID, and ISE Node (exception Health Summary report).

ISE Community Resource
For a complete list of troubleshooting TechNotes, see ISE Troubleshooting TechNotes.

Cisco ISE Dashboard

The Cisco ISE dashboard, or home page (Home > Summary), is the landing page that appears after you log in to the Cisco ISE administration console. The dashboard is a centralized management console consisting of metric meters along the top of the window, with dashlets below. The default dashboards are Summary, Endpoints, Guests, Vulnerability, and Threat. Refer to the ISE Home Dashboards, on page 15 section for additional information.

Note
You should view the dashboard data only in the Primary PAN.

The dashboard’s real-time data provides an at-a-glance status of the devices and users that are accessing your network as well as the system health overview.

Note
You must have Adobe Flash Player installed in your browser to be able to view the dashlets and all the corresponding drill down pages properly.

The following options are available under Dashboard Settings:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add New Dashboard</td>
<td>You can add a new dashboard by clicking the plus sign or from Dashboard Settings on the top right of the page.</td>
</tr>
<tr>
<td></td>
<td>Note You can add maximum of 20 dashboards including the 5 default dashboards.</td>
</tr>
<tr>
<td>Rename Dashboard</td>
<td>To rename a dashboard (available only for custom dashboards):</td>
</tr>
<tr>
<td></td>
<td>2. Specify new name.</td>
</tr>
<tr>
<td></td>
<td>3. Click Apply.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Add Dashlet         | To add a dashlet:  
  1. Choose Dashboard Settings > Add Dashlet(s). 
  2. In the Add Dashlets window, click Add against the dashlets that you want to add. 
  3. Click Save.  
  Note: You can add a maximum of 9 dashlets per dashboard. |
| Export              | You can export the dashlet data as a PDF or CSV file. To do this:  
  1. Choose the required dashboard (for example, Summary) from the Cisco ISE Home page. 
  2. Choose Dashboard Settings > Export. 
  3. In the Export dialog box, choose one of the following file formats:  
     - Select the PDF format to view a snapshot of the selected dashlets. 
     - Select the CSV format to download the selected dashboard data as a ZIP file. 
  4. In the Dashlets section, select the required dashlets. 
  5. Click Export.  
  The ZIP file is named according to the selected dashboard (Example: Summary.zip). The ZIP file contains individual dashlet CSV files for the selected dashboard. Data related to each tab in a dashlet appears as separate sections in the corresponding dashlet CSV file.  
  When you export a custom dashboard, the file is exported with the same name. For example, if you export a custom dashboard, named MyDashboard, then the exported file name is MyDashboard. |
| Layout Template     | You can change the layout of the template in which the dashlets are displayed. To change the layout:  
  1. Choose Dashboard Settings > Layout Template. 
  2. Select the desired layout from the options available. |
The following options are available under Manage Dashboards:

- Mark as Default Dashboard—Use this option to set a dashboard as your default dashboard (home page)
- Reset all Dashboards—Use this option to reset all the dashboards to their original settings

You can delete a dashboard that you have created by clicking the close (x) icon next to the custom dashboard.

**Note**

You cannot rename or delete a default dashboard.

All the dashlets have a toolbar on the top right, which has the following options:

1. Detach—To view a dashlet in a separate window.
2. Refresh—To refresh a dashlet.
3. Remove—To remove a dashlet from the dashboard.

You can drag and drop the dashlet using the gripper icon present in the top left corner of the dashlet.

Quick Filter in Alarms Dashlet—You can filter alarms based on the severity such as Critical, Warning, and Info. The Alarms dashlet is found on the Home page, and contains the Filter drop-down, which contains a Quick Filter to search for alarms based on the severity.

### NPF Event Flow Process

The NPF authentication and authorization event flow uses the process described in the following table:

<table>
<thead>
<tr>
<th>Process Stage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NAD performs an authorization or flex authorization.</td>
</tr>
<tr>
<td>2</td>
<td>An unknown agentless identity is profiled with web authorization.</td>
</tr>
<tr>
<td>3</td>
<td>RADIUS server authenticates and authorizes the identity.</td>
</tr>
<tr>
<td>4</td>
<td>Authorization is provisioned for the identity at the port.</td>
</tr>
<tr>
<td>5</td>
<td>Unauthorized endpoint traffic is dropped.</td>
</tr>
</tbody>
</table>
User Roles and Permissions for Monitoring and Troubleshooting Capabilities

Monitoring and troubleshooting capabilities are associated with default user roles. The tasks you are allowed to perform are directly related to your assigned user role.

Data Stored in Monitoring Database

The Cisco ISE monitoring service collects and stores data in a specialized monitoring database. The rate and amount of data utilized to monitor network functions may require a node dedicated solely to monitoring. If your Cisco ISE network collects logging data at a high rate from Policy Service nodes or network devices, a Cisco ISE node dedicated to monitoring is recommended.

To manage the information stored in the Monitoring database, you are required to perform full and incremental backups of the database. This includes purging unwanted data, and then restoring the database.

Related Topics
   Monitoring Database, on page 901

Device Configuration for Monitoring

The Monitoring node receives and uses data from devices on the network to populate the dashboard display. To enable communication between the Monitoring node and the network devices, switches and Network Access Devices (NADs) must be configured properly.

Troubleshooting the Anyconnect Agent Download Issues

If a PSN goes down during Network setup assistance while downloading anyconnect, the user must re-download AC agent from the client provisioning portal and run the complete flow again.

Troubleshooting the Profiler Feed

If the Test was able to connect to the Cisco Feed server, then you will see a popup that says that the test connection was successful.

If the connection failed, the test button area will contain a response from the server, similar to the following example, where the bold part of the message shows the important part of the message:


Here are some possible error messages and actions to take:

• Unable to find valid certification path to requested target - The certificate that the Feed server used is not valid. Verify that you have enabled the Verisign certificates.

• No route to host - Verify that you have a working connection to an outside network from the ISE server.
- UnknownHostException (at the beginning of the error message) - Verify that you have a working connection to an outside network from the ISE server.

Posture Compliance

The Posture Compliance dashlet provides information on the users who are accessing the network and whether they meet posture compliance. Data is shown on the devices that are currently connected to the network. The stack bars show noncompliance statistics that are arranged according to operating system and other criteria. Sparklines represent the percentage of compliant versus noncompliant posture attempts.

Check Posture Compliance

Step 1 Go to the Cisco ISE Dashboard.
Step 2 In the Posture Compliance dashlet, hover your cursor over a stack bar or sparkline. A tooltip provides detailed information.
Step 3 Expand the data categories for more information.
Step 4 Expand the Posture Compliance dashlet. A detailed real-time report appears.

Note You can view the posture compliance report in the Context Visibility page. The Context Visibility page (Context Visibility > Endpoints > Compliance) displays different charts based on the compliance status, location, type of endpoints and status trend.

You might see posture status for endpoints that do not have any active sessions. For example, if the last known posture status for an endpoint is Compliant, the status remains Compliant in the Context Visibility page until the next update is received for the endpoint, even if the endpoint session is terminated. The posture status is retained in the Context Visibility page until that endpoint is deleted or purged.

SNMP Traps To Monitor Cisco ISE Processes

SNMP traps help you to monitor the status of Cisco ISE processes. Without accessing the Cisco ISE server, if you want to monitor the Cisco ISE processes, you can configure a MIB browser as an SNMP host in Cisco ISE. You can then monitor the status of Cisco ISE processes from the MIB browser.

Cisco ISE uses a cron job to trigger these traps. After you configure the SNMP host command from the CLI, a cron job runs every five minutes and monitors the Cisco ISE processes. The first time you configure the SNMP host, you can see that separate traps are received in the SNMP server for each process that is running in Cisco ISE, irrespective of its status.

You can verify that the configured SNMP server is able to receive the traps that are sent from Cisco ISE. After that, traps are sent from Cisco ISE only when there is a change in the process status. You can view the SNMP traps using the traps receiver in a MIB browser.
Cisco ISE sends traps using the OID of hrSWRunName that belongs to the HOST-RESOURCES MIB and sets the OID value as `<PROCESS NAME> - <PROCESS STATUS>`.

For instance, runtime - running.

Cisco ISE supports SNMPv1, SNMPv2c, and SNMPv3.

Cisco ISE sends the following generic system traps if you configure the SNMP host from the CLI:

- **Cold start**—When the device reboots
- **Linkup**—When Ethernet interface is up
- **Linkdown**—When Ethernet interface is down
- **Authentication failure**—When the community strings do not match

Cisco ISE sends traps for the following status to the configured SNMP server:

- **Process Start** (monitored state)
- **Process Stop** (not monitored state)
- **Execution Failed**—When the process state changes from “monitored” to “execution failed,” a trap is sent.
- **Does not exists**—When the process state changes from “monitored” to “does not exists,” a trap is sent.
- **Disk utilization**—When a Cisco ISE partition reaches its threshold disk utilization limit (the trap is sent when the configured amount of free space is reached).

In the SNMP server, for every object, a unique object ID is generated and a value is assigned to the OID. You can find the object with its OID value in the SNMP server. The OID value for a running trap is “running,” and the OID value for not monitored, does not exist, and execution failed traps is “stopped.”

To stop Cisco ISE from sending SNMP traps to the SNMP server, remove the SNMP configuration from the Cisco ISE CLI. This operation stops sending SNMP traps and polling from the SNMP manager.

Refer to the Cisco Identity Services Engine CLI Reference Guide for information on the `snmp-server host` and `snmp-server trap` commands.

**Note**

ISE does not have any MIB for process status or disk utilization. Cisco ISE uses OID HOST-RESOURCES-MIB::hrSWRunName for sending SNMP trap. You cannot use snmp walk or snmp get command to query the process status or disk utilization.

<table>
<thead>
<tr>
<th>OID</th>
<th>SNMP Trap</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Trap Events for Disk Utilization</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.4.1.2021.9.1.9</td>
<td>UCD_SNMP_OID:dskPercent</td>
</tr>
<tr>
<td>1.3.6.1.4.1.2021.9.1.2</td>
<td>UCD_SNMP_OID:dskPath</td>
</tr>
<tr>
<td>SNMP Trap Notification for Process Status</td>
<td></td>
</tr>
<tr>
<td>1.3.6.1.2.1.25.4.2.1.2</td>
<td>HOST-RESOURCES-MIB:hrSWRunName</td>
</tr>
</tbody>
</table>
**SNMP TrapOID**

Other SNMP Traps whose notification events are communicated by default. For more information, refer to the following URL: [http://oidref.com/1.3.6.1.6.3.1.1.5.](http://oidref.com/1.3.6.1.6.3.1.1.5.)

<table>
<thead>
<tr>
<th>OID</th>
<th>SNMP Trap</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.6.3.1.1.5.1</td>
<td>ColdStart</td>
</tr>
<tr>
<td>1.3.6.1.6.3.1.1.5.5</td>
<td>AuthenticationFailure</td>
</tr>
</tbody>
</table>

**SNMP Trap Events Sent from the Network to Cisco ISE**

<table>
<thead>
<tr>
<th>OID</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.1.6.3.1.1.5.3</td>
<td>linkUp event</td>
</tr>
<tr>
<td>1.3.6.1.6.3.1.1.5.4</td>
<td>linkDown event</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.0.3</td>
<td>Cisco Link Up event</td>
</tr>
<tr>
<td>1.3.6.1.2.1.11.0.2</td>
<td>Cisco Link Down event</td>
</tr>
<tr>
<td>1.3.6.1.4.1.9.9.215.2.0.1</td>
<td>Cisco Mac Change Notification</td>
</tr>
<tr>
<td>1.3.6.1.4.1.9.9.215.2.0.2</td>
<td>Cisco Mac Move Notification</td>
</tr>
</tbody>
</table>

Using Cisco Mac Change Notification SNMP Trap OIDs, the following attributes: MAC-Address, Timestamp, MacStatus, Vlan, and dot1dBasePort are used for creating an Endpoint.

Using the SNMP Trap Event CommandResponderEvent, you can read the peerAddress, which is the address of the Network Device. You can read the IfIndex, Vlan, and MAC-Address attributes from the CommandResponderEvent PDU command variables and use them to perform SNMP Query on the Network to fetch the CDP attributes and add them to the Endpoint.

## Cisco ISE Alarms

Alarms notify you of critical conditions on a network and are displayed in the Alarms dashlet. They also provide information on system activities, such as data purge events. You can configure how you want to be notified about system activities, or disable them entirely. You can also configure the threshold for certain alarms.

Most alarms do not have an associated schedule and are sent immediately after an event occurs. At any given point in time, only the latest 15,000 alarms are retained.

If the event re-occurs, then the same alarms are suppressed for about an hour. During the time that the event re-occurs, depending up on the trigger, it may take about an hour for the alarms to re-appear.

The following table lists all the Cisco ISE alarms, descriptions and their resolution.

### Table 70: Cisco ISE Alarms

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm Description</th>
<th>Alarm Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative and Operational Audit Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deployment Upgrade Failure</td>
<td>An upgrade has failed on an ISE node.</td>
<td>Check the ADE.log on the failed node for upgrade failure reason and corrective actions.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Alarm Description</td>
<td>Alarm Resolution</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Upgrade Bundle Download failure</td>
<td>An upgrade bundle download has failed on an ISE node.</td>
<td>Check the ADE.log on the failed node for upgrade failure reason and corrective actions.</td>
</tr>
<tr>
<td>SXP Connection Failure</td>
<td>SXP Connection has failed.</td>
<td>Verify that the SXP service is running. Check peer for compatibility.</td>
</tr>
<tr>
<td>Cisco profile applied to all devices</td>
<td>Network device profiles define the capabilities of network access devices, such as MAB, Dot1X, CoA, Web Redirect. As part of the ISE 2.0 upgrade, the default Cisco network device profile was applied to all network devices.</td>
<td>Consider editing the configuration of non-Cisco network devices to assign the appropriate profile.</td>
</tr>
<tr>
<td>Secure LDAP connection reconnect due to CRL found revoked certificate</td>
<td>CRL check result is that the certificate used for LDAP connection is revoked.</td>
<td>Check the CRL configuration and verify that it is valid. Check that the LDAP server certificate and its issuer certificates are not revoked. If revoked issue new certificate and install it on LDAP server.</td>
</tr>
<tr>
<td>Secure LDAP connection reconnect due to OCSP found revoked certificate</td>
<td>OCSP check result is that the certificate used for LDAP connection is revoked.</td>
<td>Check the OCSP configuration and verify that it is valid. Check that the LDAP server certificate and its issuer certificates are not revoked. If revoked issue new certificate and install it on LDAP server.</td>
</tr>
<tr>
<td>Secure syslog connection reconnect due to CRL found revoked certificate</td>
<td>CRL check result is that the certificate used for syslog connection is revoked.</td>
<td>Check the CRL configuration and verify that it is valid. Check that the syslog server certificate and its issuer certificates are not revoked. If revoked issue new certificate and install it on syslog server.</td>
</tr>
<tr>
<td>Secure syslog connection reconnect due to OCSP found revoked certificate</td>
<td>OCSP check result is that the certificate used for syslog connection is revoked.</td>
<td>Check the OCSP configuration and verify that it is valid. Check that the syslog server certificate and its issuer certificates are not revoked. If revoked issue new certificate and install it on syslog server.</td>
</tr>
<tr>
<td>Administrator account Locked/Disabled</td>
<td>Administrator account is locked or disabled due to password expiration or incorrect login attempts. For more details, refer to the administrator password policy.</td>
<td>Administrator password can be reset by another administrator using the GUI or CLI.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Alarm Description</td>
<td>Alarm Resolution</td>
</tr>
<tr>
<td>------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>ERS identified deprecated URL</td>
<td>ERS identified deprecated URL</td>
<td>The request URL is deprecated and it is recommended to avoid using it.</td>
</tr>
<tr>
<td>ERS identified out-dated URL</td>
<td>ERS identified out-dated URL</td>
<td>The requested URL is outdated and it is recommended to use a newer one. This URL will not be removed in future releases.</td>
</tr>
<tr>
<td>ERS request content-type header is outdated</td>
<td>ERS request content-type header is outdated.</td>
<td>The request resource version stated in the request content-type header is outdated. That means that the resource schema has been modified. One or more attributes may have been added or removed. To overcome that with the outdated schema, the ERS Engine will use default values.</td>
</tr>
<tr>
<td>ERS XML input is a suspect for XSS or Injection attack</td>
<td>ERS XML input is a suspect for XSS or Injection attack.</td>
<td>Please review your xml input.</td>
</tr>
</tbody>
</table>
| Backup Failed | The ISE backup operation failed. | Check the network connectivity between Cisco ISE and the repository. Ensure that:  
• The credentials used for the repository is correct.  
• There is sufficient disk space in the repository.  
• The repository user has write privileges. |
<p>| CA Server is down | CA server is down. | Check to make sure that the CA services are up and running on the CA server. |
| CA Server is Up | CA server is up. | A notification to inform the administrator that the CA server is up. |</p>
<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm Description</th>
<th>Alarm Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Expiration</td>
<td>This certificate will expire soon. When it expires, Cisco ISE may fail to establish secure communication with clients.</td>
<td>Replace the certificate. For a trust certificate, contact the issuing Certificate Authority (CA). For a CA-signed local certificate, generate a CSR and have the CA create a new certificate. For a self-signed local certificate, use Cisco ISE to extend the expiration date. You can delete the certificate if it is no longer used.</td>
</tr>
<tr>
<td>Certificate Revoked</td>
<td>Administrator has revoked the certificate issued to an Endpoint by the Internal CA.</td>
<td>Go through the BYOD flow from the beginning to be provisioned with a new certificate.</td>
</tr>
<tr>
<td>Certificate Provisioning</td>
<td>Certificate provisioning initialization failed</td>
<td>More than one certificate found with the same value of CN (CommonName) attribute in the subject, cannot build certificate chain. Check all the certificates in the system including those from the SCEP server.</td>
</tr>
<tr>
<td>Initialization Error</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate Replication Failed</td>
<td>Certificate replication to secondary node failed</td>
<td>The certificate is not valid on the secondary node, or there is some other permanent error condition. Check the secondary node for a pre-existing, conflicting certificate. If found, delete the pre-existing certificate on the secondary node, and export the new certificate on the primary, delete it, and import it in order to reattempt replication.</td>
</tr>
<tr>
<td>Certificate Replication</td>
<td>Certificate replication to secondary node temporarily failed</td>
<td>The certificate was not replicated to a secondary node due to a temporary condition such as a network outage. The replication will be retried until it succeeds.</td>
</tr>
<tr>
<td>Temporarily Failed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certificate Expired</td>
<td>This certificate has expired. Cisco ISE may fail to establish secure communication with clients. Node-to-node communication may also be affected.</td>
<td>Replace the certificate. For a trust certificate, contact the issuing Certificate Authority (CA). For a CA-signed local certificate, generate a CSR and have the CA create a new certificate. For a self-signed local certificate, use Cisco ISE to extend the expiration date. You can delete the certificate if it is no longer used.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Alarm Description</td>
<td>Alarm Resolution</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Certificate Request Forwarding</td>
<td>Certificate request forwarding failed.</td>
<td>Make sure that the certification request coming in matches with attributes from the sender.</td>
</tr>
<tr>
<td>Failed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration Changed</td>
<td>Cisco ISE configuration is updated.</td>
<td>Check if the configuration change is expected.</td>
</tr>
<tr>
<td>CRL Retrieval Failed</td>
<td>Unable to retrieve CRL from the server.</td>
<td>Ensure that the download URL is correct and is available for the service.</td>
</tr>
<tr>
<td>DNS Resolution Failure</td>
<td>DNS resolution failed on the node.</td>
<td>Check if the DNS server configured by the command <code>ip name-server</code> is reachable. If you get the alarm as 'DNS Resolution failed for CNAME &lt;hostname of the node&gt;', then ensure that you create CNAME RR along with the A record for each Cisco ISE node.</td>
</tr>
<tr>
<td>Firmware Update Required</td>
<td>A firmware update is required on this host.</td>
<td>Contact Cisco Technical Assistance Center to obtain firmware update.</td>
</tr>
<tr>
<td>Insufficient Virtual Machine</td>
<td>Virtual Machine (VM) resources such as CPU, RAM, Disk Space, or IOPS are insufficient on this host.</td>
<td>Ensure that a minimum requirements for the VM host, as specified in the Cisco ISE Hardware Installation Guide.</td>
</tr>
<tr>
<td>Resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NTP Service Failure</td>
<td>The NTP service is down on this node.</td>
<td>This could be because there is a large time difference between NTP server and Cisco ISE node( more than 1000s). Ensure that your NTP server is working properly and use the <code>ntp server &lt;servername&gt;</code> CLI command to restart the NTP service and fix the time gap.</td>
</tr>
<tr>
<td>NTP Sync Failure</td>
<td>All the NTP servers configured on this node are unreachable.</td>
<td>Execute <code>show ntp</code> command from the CLI for troubleshooting. Ensure that the NTP servers are reachable from Cisco ISE. If NTP authentication is configured, ensure that the key ID and value matches with that of the server.</td>
</tr>
<tr>
<td>No Configuration Backup Scheduled</td>
<td>No Cisco ISE configuration backup is scheduled.</td>
<td>Create a schedule for configuration backup.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Alarm Description</td>
<td>Alarm Resolution</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Operations DB Purge Failed</td>
<td>Unable to purge older data from the operations database. This could occur if M&amp;T nodes are busy.</td>
<td>Check the Data Purging Audit report and ensure that the used_space is lesser than the threshold_space. Login to M&amp;T nodes using CLI and perform the purge operation manually.</td>
</tr>
<tr>
<td>Profiler SNMP Request Failure</td>
<td>Either the SNMP request timed out or the SNMP community or user authentication data is incorrect.</td>
<td>Ensure that SNMP is running on the NAD and verify that SNMP configuration on Cisco ISE matches with NAD.</td>
</tr>
<tr>
<td>Replication Failed</td>
<td>The secondary node failed to consume the replicated message.</td>
<td>Login to the Cisco ISE GUI and perform a manual syncup from the deployment page. De-register and register back the affected Cisco ISE node.</td>
</tr>
<tr>
<td>Restore Failed</td>
<td>Cisco ISE restore operation failed.</td>
<td>Ensure the network connectivity between Cisco ISE and the repository. Ensure that the credentials used for the repository is correct. Ensure that the backup file is not corrupted. Execute the <code>reset-config</code> command from the CLI and restore the last known good backup.</td>
</tr>
<tr>
<td>Patch Failure</td>
<td>A patch process has failed on the server.</td>
<td>Re-install the patch process on the server.</td>
</tr>
<tr>
<td>Patch Success</td>
<td>A patch process has succeeded on the server.</td>
<td>-</td>
</tr>
<tr>
<td>External MDM Server API Version Mismatch</td>
<td>External MDM server API version does not match with what is configured in Cisco ISE.</td>
<td>Ensure that the MDM server API version is the same as what is configured in Cisco ISE. Update Cisco ISE MDM server configuration if needed.</td>
</tr>
<tr>
<td>External MDM Server Connection Failure</td>
<td>Connection to the external MDM server failed.</td>
<td>Ensure that the MDM server is up and Cisco ISE-MDM API service is running on the MDM server.</td>
</tr>
<tr>
<td>External MDM Server Response Error</td>
<td>External MDM Server response error.</td>
<td>Ensure that the Cisco ISE-MDM API service is properly running on the MDM server.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Alarm Description</td>
<td>Alarm Resolution</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Replication Stopped</td>
<td>ISE node could not replicate configuration data from the PAN.</td>
<td>Login to the Cisco ISE GUI to perform a manual syncup from the deployment page or de-register and register back the affected ISE node with required field.</td>
</tr>
<tr>
<td>Endpoint certificates expired</td>
<td>Endpoint certificates were marked expired by daily scheduled job.</td>
<td>Please re-enroll the endpoint device to get a new endpoint certificate.</td>
</tr>
<tr>
<td>Endpoint certificates purged</td>
<td>Expired endpoint certificates were purged by daily scheduled job.</td>
<td>No action needed - this was an administrator-initiated cleanup operation.</td>
</tr>
<tr>
<td>Endpoints Purge Activities</td>
<td>Purge activities on endpoints for the past 24 hours. This alarm is triggered at mid-night.</td>
<td>Review the purge activities under Operations &gt; Reports &gt; Endpoints and Users &gt; Endpoint Purge Activities</td>
</tr>
<tr>
<td>Slow Replication Error</td>
<td>Slow or a stuck replication is detected .</td>
<td>Please verify that the node is reachable and part of the deployment.</td>
</tr>
<tr>
<td>Slow Replication Info</td>
<td>Slow or a stuck replication is detected .</td>
<td>Please verify that the node is reachable and part of the deployment.</td>
</tr>
<tr>
<td>Slow Replication Warning</td>
<td>Slow or a stuck replication is detected .</td>
<td>Please verify that the node is reachable and part of the deployment.</td>
</tr>
<tr>
<td>PAN Auto Failover - Failover Failed</td>
<td>Promotion request to the Secondary administration node failed.</td>
<td>Please refer to the alarm details for further action.</td>
</tr>
<tr>
<td>PAN Auto Failover - Failover Triggered</td>
<td>Successfully triggered the failover of the Secondary Administration node to Primary role.</td>
<td>Wait for promotion of secondary PAN to complete and bring up the old primary PAN.</td>
</tr>
<tr>
<td>PAN Auto Failover - Health Check Inactivity</td>
<td>PAN did not receive the health check monitoring request from the designated monitoring node.</td>
<td>Please verify if the reported monitoring node is down or out-of-sync and trigger a manual sync if needed.</td>
</tr>
<tr>
<td>PAN Auto Failover - Invalid Health Check</td>
<td>Invalid health check monitoring request received for auto-failover.</td>
<td>Please verify if the health check monitoring node is out-of-sync and trigger a manual sync if needed.</td>
</tr>
<tr>
<td>PAN Auto Failover - Primary Administration Node Down</td>
<td>Primary Admin node is down or is not reachable from the monitoring node.</td>
<td>Bring up the PAN or wait for failover to happen.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Alarm Description</td>
<td>Alarm Resolution</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PAN Auto Failover - Rejected</td>
<td>Secondary administration node rejected the promotion request made by the health check monitor node.</td>
<td>Refer to the alarm details for further action.</td>
</tr>
<tr>
<td>Failover Attempt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EST Service is down</td>
<td>EST Service is down.</td>
<td>Make sure that the CA and EST services are up and running and Certificate services endpoint Sub CA certificate chain is complete.</td>
</tr>
<tr>
<td>EST Service is up</td>
<td>EST Service is up.</td>
<td>A notification to inform the administrator that the EST service is up.</td>
</tr>
<tr>
<td>Smart Call Home Communication</td>
<td>Smart Call Home messages were not sent successfully.</td>
<td>Ensure that there is network connectivity between Cisco ISE and Cisco systems.</td>
</tr>
<tr>
<td>Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telemetry Communication Failure</td>
<td>Telemetry messages were not sent successfully.</td>
<td>Ensure that there is network connectivity between Cisco ISE and Cisco systems.</td>
</tr>
<tr>
<td>Adapter not reachable</td>
<td>Cisco ISE cannot connect to the adapter.</td>
<td>Check the adapter logs for more details about the failure.</td>
</tr>
<tr>
<td>Adapter Error</td>
<td>Adapter has encountered an error.</td>
<td>Check the description of the alarm.</td>
</tr>
<tr>
<td>Adapter Connection Failed</td>
<td>The adapter cannot connect to the source server.</td>
<td>Ensure that the source server is reachable.</td>
</tr>
<tr>
<td>Adapter Stopped Due to Error</td>
<td>The adapter has encountered an error and is not in the desired state.</td>
<td>Ensure that the adapter configuration is correct and the source server is reachable. Refer to the adapter logs for more details about the error.</td>
</tr>
<tr>
<td>Service Component Error</td>
<td>The service component has encountered an error.</td>
<td>Check the description of the alarm.</td>
</tr>
<tr>
<td>Service Component Info</td>
<td>The service component has sent a notification.</td>
<td>None.</td>
</tr>
<tr>
<td>ISE Services</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Excessive TACACS Authentication</td>
<td>The ISE Policy Service nodes are experiencing higher than expected rate of TACACS Authentications.</td>
<td>Check the re-auth timer in the network devices. Check the network connectivity of the ISE infrastructure.</td>
</tr>
<tr>
<td>Attempts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Alarm Description</td>
<td>Alarm Resolution</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Excessive TACACS Authentication Failed Attempts</td>
<td>The ISE Policy Service nodes are experiencing higher than expected rate of Failed TACACS Authentications.</td>
<td>Check the authentication steps to identify the root cause. Check the ISE/NAD configuration for Identity and Secret mismatch.</td>
</tr>
<tr>
<td>MSE Location Server accessible again</td>
<td>MSE Location Server is accessible again.</td>
<td>None.</td>
</tr>
<tr>
<td>MSE Location Server not accessible.</td>
<td>MSE Location Server is not accessible or is down.</td>
<td>Please check if MSE Location Server is up and running and is accessible from ISE node(s).</td>
</tr>
<tr>
<td>AD Connector had to be restarted</td>
<td>AD Connector stopped unexpectedly and had to be restarted.</td>
<td>If this issue persists, contact the Cisco TAC for assistance.</td>
</tr>
<tr>
<td>Active Directory forest is unavailable</td>
<td>Active Directory forest GC (Global Catalog) is unavailable, and cannot be used for authentication, authorization and group and attribute retrieval.</td>
<td>Check DNS configuration, Kerberos configuration, error conditions, and network connectivity.</td>
</tr>
<tr>
<td>Authentication domain is unavailable</td>
<td>Authentication domain is unavailable, and cannot be used for authentication, authorization and group and attribute retrieval.</td>
<td>Check DNS configuration, Kerberos configuration, error conditions, and network connectivity.</td>
</tr>
<tr>
<td>ISE Authentication Inactivity</td>
<td>Cisco ISE policy service nodes are not receiving authentication requests from the network devices.</td>
<td>Check the ISE/NAD configuration. Check the network connectivity of the ISE/NAD infrastructure.</td>
</tr>
<tr>
<td>ID Map. Authentication Inactivity</td>
<td>No User Authentication events were collected by the Identity Mapping service in the last 15 minutes.</td>
<td>If this is a time when User Authentications are expected (e.g. work hours), then check the connection to Active Directory domain controllers.</td>
</tr>
<tr>
<td>COA Failed</td>
<td>Network device has denied the Change of Authorization (CoA) request issued by Cisco ISE policy service nodes.</td>
<td>Ensure that the network device is configured to accept Change of Authorization (CoA) from Cisco ISE. Ensure if CoA is issued on a valid session.</td>
</tr>
<tr>
<td>Configured nameserver is down</td>
<td>Configured nameserver is down or unavailable.</td>
<td>Check DNS configuration and network connectivity.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Alarm Description</td>
<td>Alarm Resolution</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Supplicant Stopped Responding</td>
<td>Cisco ISE sent last message to the client 120 seconds ago but there is no response from the client.</td>
<td>Verify that the supplicant is configured properly to conduct a full EAP conversation with Cisco ISE. Verify that NAS is configured properly to transfer EAP messages to/from the supplicant. Verify that the supplicant or NAS does not have a short timeout for EAP conversation.</td>
</tr>
<tr>
<td>Excessive Authentication Attempts</td>
<td>Cisco ISE policy service nodes are experiencing higher than expected rate of authentications.</td>
<td>Check the re-auth timer in the network devices. Check the network connectivity of the Cisco ISE infrastructure. Once the threshold is met, the Excessive Authentication Attempts and Excessive Failed Attempts alarms are triggered. The numbers displayed next to the Description column are the total number of authentications that are authenticated or failed against Cisco ISE in last 15 minutes.</td>
</tr>
<tr>
<td>Excessive Failed Attempts</td>
<td>Cisco ISE policy service nodes are experiencing higher than expected rate of failed authentications.</td>
<td>Check the authentication steps to identify the root cause. Check the Cisco ISE/NAD configuration for identity and secret mismatch. Once the threshold is met, the Excessive Authentication Attempts and Excessive Failed Attempts alarms are triggered. The numbers displayed next to the Description column are the total number of authentications that are authenticated or failed against Cisco ISE in last 15 minutes.</td>
</tr>
<tr>
<td>AD: Machine TGT refresh failed</td>
<td>ISE server TGT (Ticket Granting Ticket) refresh has failed; it is used for AD connectivity and services.</td>
<td>Check that the ISE machine account exists and is valid. Also check for possible clock skew, replication, Kerberos configuration and/or network errors.</td>
</tr>
<tr>
<td>AD: ISE account password update failed</td>
<td>ISE server has failed to update it's AD machine account password.</td>
<td>Check that the ISE machine account password is not changed and that the machine account is not disabled or restricted. Check the connectivity to KDC.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Alarm Description</td>
<td>Alarm Resolution</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Joined domain is unavailable</td>
<td>Joined domain is unavailable, and cannot be used for authentication, authorization and group and attribute retrieval.</td>
<td>Check DNS configuration, Kerberos configuration, error conditions, and network connectivity.</td>
</tr>
<tr>
<td>Identity Store Unavailable</td>
<td>Cisco ISE policy service nodes are unable to reach the configured identity stores.</td>
<td>Check the network connectivity between Cisco ISE and identity store.</td>
</tr>
<tr>
<td>Misconfigured Network Device Detected</td>
<td>Cisco ISE has detected too many RADIUS accounting information from NAS</td>
<td>Too many duplicate RADIUS accounting information has been sent to ISE from NAS. Configure NAS with accurate accounting frequency.</td>
</tr>
<tr>
<td>Misconfigured Supplicant Detected</td>
<td>Cisco ISE has detected mis-configured supplicant on the network</td>
<td>Ensure that the configuration on Supplicant is correct.</td>
</tr>
<tr>
<td>No Accounting Start</td>
<td>Cisco ISE policy service nodes have authorized a session but did not receive accounting start from the network device.</td>
<td>Ensure that RADIUS accounting is configured on the network device. Check the network device configuration for local authorization.</td>
</tr>
<tr>
<td>Unknown NAD</td>
<td>Cisco ISE policy service nodes are receiving authentication requests from a network device that is not configured in Cisco ISE.</td>
<td>Check if the network device is a genuine request and add it to the configuration. Ensure that the secret matches.</td>
</tr>
<tr>
<td>SGACL Drops</td>
<td>Secure Group Access (SGACL) drops occurred. This occurs if a Trustsec capable device drops packets due to SGACL policy violations.</td>
<td>Run the RBACL drop summary report and review the source causing the SGACL drops. Issue a CoA to the offending source to reauthorize or disconnect the session.</td>
</tr>
<tr>
<td>RADIUS Request Dropped</td>
<td>The authentication/accounting request from a NAD is silently discarded. This may occur due to unknown NAD, mismatched shared secrets, or invalid packet content per RFC.</td>
<td>Check that the NAD/AAA client has a valid configuration in Cisco ISE. Check whether the shared secrets on the NAD/AAA client and Cisco ISE matches. Ensure that the AAA client and the network device, have no hardware problems or problems with RADIUS compatibility. Also ensure that the network that connects the device to Cisco ISE has no hardware problems.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Alarm Description</td>
<td>Alarm Resolution</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EAP Session Allocation Failed</td>
<td>A RADIUS request was dropped due to reaching EAP sessions limit. This condition can be caused by too many parallel EAP authentication requests.</td>
<td>Wait for a few seconds before invoking another RADIUS request with new EAP session. If system overload continues to occur, try restarting the ISE Server.</td>
</tr>
<tr>
<td>RADIUS Context Allocation Failed</td>
<td>A RADIUS request was dropped due to system overload. This condition can be caused by too many parallel authentication requests.</td>
<td>Wait for a few seconds before invoking a new RADIUS request. If system overload continues to occur, try restarting the ISE Server.</td>
</tr>
<tr>
<td>AD: ISE machine account does not have the required privileges to fetch groups</td>
<td>Cisco ISE machine account does not have the required privileges to fetch groups.</td>
<td>Check if the Cisco ISE machine account has rights to fetch user groups in Active Directory.</td>
</tr>
</tbody>
</table>

**System Health**

<table>
<thead>
<tr>
<th>Alarm Name</th>
<th>Alarm Description</th>
<th>Alarm Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Disk I/O Utilization</td>
<td>Cisco ISE system is experiencing high disk I/O utilization.</td>
<td>Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load.</td>
</tr>
<tr>
<td>High Disk Space Utilization</td>
<td>Cisco ISE system is experiencing high disk space utilization.</td>
<td>Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load.</td>
</tr>
<tr>
<td>High Load Average</td>
<td>Cisco ISE system is experiencing high load average.</td>
<td>Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load. If the High Load Average alarm is seen against 2:00 a.m. time stamps for Primary and Secondary MNT nodes, note that CPU usage might be high due to DBMS stats being run at that hour. CPU usage will be back to normal when the DBMS stats is complete.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Alarm Description</td>
<td>Alarm Resolution</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>High Memory Utilization</td>
<td>Cisco ISE system is experiencing high memory utilization.</td>
<td>Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load.</td>
</tr>
<tr>
<td>High Operations DB Usage</td>
<td>Cisco ISE monitoring nodes are experiencing higher volume of syslog data than expected.</td>
<td>Check and reduce the purge configuration window for the operations data.</td>
</tr>
<tr>
<td>High Authentication Latency</td>
<td>Cisco ISE system is experiencing high authentication latency.</td>
<td>Check if the system has sufficient resources. Check the actual amount of work on the system for example, number of authentications, profiler activity etc. Add additional server to distribute the load.</td>
</tr>
<tr>
<td>Health Status Unavailable</td>
<td>The monitoring node has not received health status from the Cisco ISE node.</td>
<td>Ensure that Cisco ISE nodes are up and running. Ensure that Cisco ISE nodes are able to communicate with the monitoring nodes.</td>
</tr>
<tr>
<td>Process Down</td>
<td>One of the Cisco ISE processes is not running.</td>
<td>Restart the Cisco ISE application.</td>
</tr>
<tr>
<td>Profiler Queue Size Limit Reached</td>
<td>The ISE Profiler queue size limit has been reached. Events received after reaching the queue size limit will be dropped.</td>
<td>Check if the system has sufficient resources, and ensure EndPoint attribute filter is enabled.</td>
</tr>
<tr>
<td>OCSP Transaction Threshold Reached</td>
<td>The OCSP transaction threshold has been reached. This alarm is triggered when internal OCSP service reach high volume traffic.</td>
<td>Please check if the system has sufficient resources.</td>
</tr>
<tr>
<td>Licensing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>License About to Expire</td>
<td>License installed on the Cisco ISE nodes are about to expire.</td>
<td>View the Licencing page in Cisco ISE to view the license usage.</td>
</tr>
<tr>
<td>License Expired</td>
<td>License installed on the Cisco ISE nodes has expired.</td>
<td>Contact Cisco Accounts team to purchase new licenses.</td>
</tr>
<tr>
<td>License Violation</td>
<td>Cisco ISE nodes have detected that you are exceeding or about to exceed the allowed license count.</td>
<td>Contact Cisco Accounts team to purchase additional licenses.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Alarm Description</td>
<td>Alarm Resolution</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>--------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Smart Licensing Authorization Expired</td>
<td>Authorization for Smart Licensing has expired.</td>
<td>Refer to the Cisco ISE License Administration page to manually renew registration for Smart Licensing or check your network connectivity with Cisco Smart Software Manager. Contact your Cisco partner if the issue persists.</td>
</tr>
<tr>
<td>Smart Licensing Authorization Renewal Failure</td>
<td>Renewal of Authorization with Cisco Smart Software Manager has failed.</td>
<td>Refer to the Cisco ISE License Administration page to manually renew authorization with Cisco Smart Software Manager using the Refresh button in the Licenses table. Contact your Cisco partner if issue persists.</td>
</tr>
<tr>
<td>Smart Licensing Authorization Renewal Success</td>
<td>Renewal of Authorization with Cisco Smart Software Manager was successful.</td>
<td>Notification to inform that authorization renewal of Cisco ISE with Cisco Smart Software Manager was successful.</td>
</tr>
<tr>
<td>Smart Licensing Communication Failure</td>
<td>Communication of Cisco ISE with Cisco Smart Software Manager has failed.</td>
<td>Check your network connectivity with Cisco Smart Software Manager. Login to Cisco Smart Software Manager or contact your Cisco partner if issue persists.</td>
</tr>
<tr>
<td>Smart Licensing Communication Restored</td>
<td>Communication of Cisco ISE with Cisco Smart Software Manager was restored.</td>
<td>Notification to inform that your network connectivity with Cisco Smart Software Manager has been restored.</td>
</tr>
<tr>
<td>Smart Licensing De-Registration Failure</td>
<td>De-Registration of Cisco ISE with Cisco Smart Software Manager has failed.</td>
<td>Refer to the Cisco ISE License Administration page for additional details. Login to Cisco Smart Software Manager or contact your Cisco partner if issue persists.</td>
</tr>
<tr>
<td>Smart Licensing De-Registration Success</td>
<td>De-Registration of Cisco ISE with Cisco Smart Software Manager was successful.</td>
<td>Notification to inform that de-registration of Cisco ISE with Cisco Smart Software Manager was successful.</td>
</tr>
<tr>
<td>Smart Licensing Disabled</td>
<td>Smart Licensing is disabled on Cisco ISE and Traditional Licensing is in use.</td>
<td>Refer to the License Administration page to enable Smart Licensing again. Refer to the admin guide or contact your Cisco partner to learn about using Smart Licensing on Cisco ISE.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Alarm Description</td>
<td>Alarm Resolution</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Smart Licensing Evaluation Period Expired</td>
<td>Evaluation period of Smart Licensing has expired.</td>
<td>Refer to the Cisco ISE License Administration page to register Cisco ISE with Cisco Smart Software Manager.</td>
</tr>
<tr>
<td>Smart Licensing HA Role changed</td>
<td>High Availability role change has occurred while using Smart Licensing.</td>
<td>Notification to inform that High Availability role of Cisco ISE has changed.</td>
</tr>
<tr>
<td>Smart Licensing Id Certificate Expired</td>
<td>Smart Licensing certificate has expired.</td>
<td>Refer to the Cisco ISE License Administration page to manually renew registration for Smart Licensing. Contact your Cisco partner if the issue persists.</td>
</tr>
<tr>
<td>Smart Licensing Id Certificate Renewal Failure</td>
<td>Registration renewal for Smart Licensing with Cisco Smart Software Manager has failed.</td>
<td>Refer to the Cisco ISE License Administration page to manually renew registration for Smart Licensing. Contact your Cisco partner if the issue persists.</td>
</tr>
<tr>
<td>Smart Licensing Id Certificate Renewal Success</td>
<td>Registration renewal for Smart Licensing with Cisco Smart Software Manager was successful.</td>
<td>Notification to inform that registration renewal with Cisco Smart Software Manager was successful.</td>
</tr>
<tr>
<td>Smart Licensing Invalid Request</td>
<td>Invalid request was made to Cisco Smart Software Manager.</td>
<td>See the Cisco ISE License Administration page for additional details. Login to Cisco Smart Software Manager or contact your Cisco partner if issue persists.</td>
</tr>
<tr>
<td>Smart Licensing Out of Compliance</td>
<td>Cisco ISE licenses are Out Of Compliance.</td>
<td>See the ISE License Administration page for additional details. Contact your partner or Cisco account team to purchase new licenses.</td>
</tr>
<tr>
<td>Smart Licensing Registration Failure</td>
<td>Registration of Cisco ISE with Cisco Smart Software Manager has failed.</td>
<td>See the ISE License Administration page for additional details. Login to Cisco Smart Software Manager or contact your Cisco partner if issue persists.</td>
</tr>
<tr>
<td>Smart Licensing Registration Successful</td>
<td>Registration of Cisco ISE with Cisco Smart Software Manager was successful.</td>
<td>Notification to inform that registration of Cisco ISE with Cisco Smart Software Manager was successful.</td>
</tr>
<tr>
<td>System Error</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Alarm Description</td>
<td>Alarm Resolution</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Log Collection Error</td>
<td>Cisco ISE monitoring collector process is unable to persist the audit logs generated from the policy service nodes.</td>
<td>This will not impact the actual functionality of the Policy Service nodes. Contact TAC for further resolution.</td>
</tr>
<tr>
<td>Scheduled Report Export Failure</td>
<td>Unable to copy the exported report (CSV file) to configured repository.</td>
<td>Verify the configured repository. If it has been deleted, add it back. If it is not available or not reachable, reconfigure the repository to a valid one.</td>
</tr>
<tr>
<td>Trustsec</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unknown SGT was provisioned</td>
<td>Unknown SGT was provisioned.</td>
<td>ISE provisioned the Unknown SGT as part of the authorization flow. Unknown SGT should not be assigned as part of a known flow.</td>
</tr>
<tr>
<td>Some TrustSec network devices do not have the latest ISE IP-SGT mapping configuration</td>
<td>Some TrustSec network devices do not have the latest ISE IP-SGT mapping configuration.</td>
<td>ISE identified some network devices that have a different IP-SGT mapping sets. Use the IP-SGT mapping Deploy option to update the devices.</td>
</tr>
<tr>
<td>TrustSec SSH connection failed</td>
<td>TrustSec SSH connection failed</td>
<td>ISE failed to establish SSH connection to a network device. Verify if the network device SSH credentials in the Network Device page are similar to the credentials configured on the network device. Check the network device enabled ssh connections from ISE (ip address).</td>
</tr>
<tr>
<td>TrustSec identified ISE was set to work with TLS versions other then 1.0</td>
<td>TrustSec identified ISE was set to work with TLS versions other then 1.0.</td>
<td>TrustSec supports only TLS version 1.0.</td>
</tr>
<tr>
<td>Trustsec PAC validation failed</td>
<td>Trustsec PAC validation failed</td>
<td>ISE could not validate a PAC which was sent by the network device. Check the Trustsec device credentials in the Network Device page and in the device CLI. Make sure the device uses a valid pac which was provisioned by the ISE server.</td>
</tr>
</tbody>
</table>
**Alarm Settings**

The following table describes the fields in the Alarm Settings page. (Administration > System > Settings > Alarm Settings)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Type</td>
<td>Choose the alarm type from the drop-down list.</td>
</tr>
<tr>
<td>Alarm Name</td>
<td>Enter the name of the alarm.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the alarm.</td>
</tr>
<tr>
<td>Suggested Actions</td>
<td>Enter any suggested action to be performed when the alarm is triggered.</td>
</tr>
<tr>
<td>Status</td>
<td>Select the status to Enable or Disable the alarm rule.</td>
</tr>
<tr>
<td>Severity</td>
<td>Use the drop-down list box to select the severity level for your alarm. Valid options are:</td>
</tr>
<tr>
<td></td>
<td>• Critical—Indicates a critical error condition.</td>
</tr>
<tr>
<td></td>
<td>• Warning—Indicates a normal but significant condition. This is the default condition.</td>
</tr>
<tr>
<td></td>
<td>• Info—Indicates an informational message.</td>
</tr>
</tbody>
</table>

Alarms are not triggered when you add users or endpoints to Cisco ISE.
Add Custom Alarms

Cisco ISE contains 12 default alarm types, such as High Memory Utilization and Configuration Changes. Cisco-defined system alarms are listed in the Alarms Settings page (Administration > System > Settings > Alarms Settings). You can only edit the system alarms.

In addition to the existing system alarms, you can add, edit, or delete custom alarms under the existing alarm types.

For each alarm type, you can create a maximum of 5 alarms and the total number of alarms is limited to 200.

To add an alarm:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose Administration &gt; System &gt; Settings &gt; Alarm Settings.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Alarm Configuration tab, click Add.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter the required details. Refer to the Alarm Settings section for more information.</td>
</tr>
</tbody>
</table>

Based on the alarm type (High Memory Utilization, Excessive RADIUS Authentication Attempts, Excessive TACACS Authentication Attempts, and so on), additional attributes are displayed in the Alarm Configuration page. For example, Object Name, Object Type, and Admin Name fields are displayed for Configuration Change alarms. You can add multiple instances of same alarm with different criteria.

| Step 4 | Click Submit. |

Cisco ISE Alarm Notifications and Thresholds

You can enable or disable Cisco ISE alarms and configure alarm notification behavior to notify you of critical conditions. For certain alarms you can configure thresholds like maximum failed attempts for Excessive Failed Attempts alarm or maximum disk utilization for High Disk Utilization alarm.

You can configure the notification settings on per-alarm basis. You can enter the email IDs of the users that need to be notified for each alarm (both system-defined and user-defined alarms).

Note

The recipient email address specified at the alarm rule level overrides the global recipient email address setting.
Enable and Configure Alarms

Step 1  Choose Administration > System > Settings > Alarm Settings.
Step 2  Select an alarm from the list of default alarms and click Edit.
Step 3  Select Enable or Disable.
Step 4  Configure alarm threshold if applicable.
Step 5  Click Submit.

Cisco ISE Alarms for Monitoring

Cisco ISE provides system alarms which notify you whenever any critical system condition occurs. Alarms that are generated by Cisco ISE are displayed in the Alarm dashlet. These notifications automatically appear in the alarm dashlet.

The Alarm dashlet displays a list of recent alarms, which you can select from to view the alarm details. You can also receive notification of alarms through e-mail and syslog messages.

View Monitoring Alarms

Step 1  Go to the Cisco ISE Dashboard.
Step 2  Click on an alarm in the Alarms dashlet. A new window opens with the alarm details and a suggested action.
Step 3  Click Refresh to refresh the alarms.
Step 4  Click Acknowledge to acknowledge selected alarms. You can select the alarms by clicking the check box available prior to the timestamp. This reduces the alarm counters (number of times an alarm is raised) when marked as read.
Step 5  Click the Details link corresponding to the alarm that you select. A new window opens with the details corresponding to the alarm that you select.

Note  The Details link corresponding to the previous alarms that were generated prior to persona change shows no data.

Log Collection

Monitoring services collect log and configuration data, store the data, and then process it to generate reports and alarms. You can view the details of the logs that are collected from any of the servers in your deployment.

Alarm Syslog Collection Location

If you configure monitoring functions to send alarm notifications as syslog messages, you need a syslog target to receive the notification. Alarm syslog targets are the destinations where alarm syslog messages are sent.
You must also have a system that is configured as a syslog server to be able to receive syslog messages. You can create, edit, and delete alarm syslog targets.

---

**Note**

Cisco ISE monitoring requires that the logging-source interface configuration use the network access server (NAS) IP address. You must configure a switch for Cisco ISE monitoring.

---

### Live Authentications

You can monitor recent RADIUS authentications as they happen from the Live Authentications page. The page displays the top 10 RADIUS authentications in the last 24 hours. This section explains the functions of the Live Authentications page.

The Live Authentications page shows the live authentication entries corresponding to the authentication events as they happen. In addition to authentication entries, this page also shows the live session entries corresponding to the events. You can also drill-down the desired session to view a detailed report corresponding to that session.

The Live Authentications page provides a tabular account of recent RADIUS authentications, in the order in which they happen. The last update shown at the bottom of the Live Authentications page shows the date of the server, time, and timezone.

When a single endpoint authenticates successfully, two entries appear in the Live Authentications page: one corresponding to the authentication record and another corresponding to the session record (pulled from session live view). Subsequently, when the device performs another successful authentication, the repeat counter corresponding to the session record is incremented. The Repeat Counter that appears in the Live Authentications page shows the number of duplicate radius authentication success messages that are suppressed.

See the Live Authentication data categories that are shown by default that are described in the Recent RADIUS Authentications section.

You can choose to view all of the columns, or to display only selected data columns. After selecting the columns that you want to appear, you can save your selections.

### Monitor Live Authentications

#### Step 1
Choose **Operations** > **RADIUS Livelog**.

#### Step 2
Select a time interval from the **Refresh** drop-down list to change the data refresh rate.

#### Step 3
Click the **Refresh** icon to manually update the data.

#### Step 4
Choose an option from the **Show** drop-down list to change the number of records that appear.

#### Step 5
Choose an option from the **Within** drop-down list to specify a time interval.

#### Step 6
Click **Add or Remove Columns** and choose the options from the drop-down list to change the columns that are shown.

#### Step 7
Click **Save** at the bottom of the drop-down list to save your modifications.

#### Step 8
Click **Show Live Sessions** to view live RADIUS sessions.
You can use the dynamic Change of Authorization (CoA) feature for the Live Sessions that allows you to dynamically control active RADIUS sessions. You can send reauthenticate or disconnect requests to a Network Access Device (NAD).

Filter Data in Live Authentications Page

With the filters in the Live Authentications page, you can filter out information that you need and troubleshoot network authentication issues quickly. You can filter records in the Authentication (live logs) page and view only those records that you are interested in. The authentication logs contain many details and filtering the authentications from a particular user or location helps you scan the data quickly. You can use several operators that are available on various fields in the Live Authentications page to filter out records based on your search criteria.

- 'abc' - Contains 'abc'
- '!abc' - Does not contain 'abc'
- '{}' - Is empty
- '!{}' - Is not empty
- 'abc*' - Starts with 'abc'
- '*abc' - Ends with 'abc'
- '!\!', '!@!', '!\{', '!\|' - Escape

The Escape option allows you to filter text with special characters (including the special characters used as filters). You must prefix the special character with a backward slash (/). For example, if you want to view the authentication records of users with identity "Employee!", enter "Employee\!" in the identity filter textbox. In this example, Cisco ISE considers the exclamation mark (!) as a literal character and not as a special character.

In addition, the Status field allows you to filter out only passed authentication records, failed authentications, live sessions, and so on. The green check mark filters all passed authentications that occurred in the past. The red cross mark filters all failed authentications. The blue i icon filters all live sessions. You can also choose to view a combination of these options.

**Step 1**
Choose **Operations > RADIUS Livelog**.

**Step 2**
Filter data based on any of the fields in the Show Live Authentications page.

You can filter the results based on passed or failed authentications, or live sessions.

Global Search for Endpoints

You can use the global search box available at the top of the Cisco ISE home page to search for endpoints. You can use any of the following criteria to search for an endpoint:

- User name
- MAC Address
- IP Address
- Authorization Profile
- Endpoint Profile
- Failure Reason
- Identity Group
- Identity Store
- Network Device name
- Network Device Type
- Operating System
- Posture Status
- Location
- Security Group
- UserType

You should enter at least three characters for any of the search criteria in the Search field to display data.

The search result provides a detailed and at-a-glance information about the current status of the endpoint, which you can use for troubleshooting. Search results display only the top 25 entries. It is recommended to use filters to narrow down the results.

The following figure shows an example of the search result.

*Figure 63: Search Result For Endpoints*

You can use any of the properties in the left panel to filter the results. You can also click on any endpoint to see more detailed information about the endpoint, such as:

- Session trace
Session Trace for an Endpoint

You can use the global search box available at the top of the Cisco ISE home page to get session information for a particular endpoint. When you search with a criteria, you get a list of endpoints. Click on any of these endpoints to see the session trace information for that endpoint. The following figure shows an example of the session trace information displayed for an endpoint.

Note

The dataset used for search is based on Endpoint ID as indexes. Therefore, when authentication occurs, it is mandatory to have Endpoint IDs for the endpoints for those authentications to include them in the search result set.
Figure 64: Session Trace of an Endpoint

You can use the clickable timeline at the top to see major authorization transitions. You can also export the results in .csv format by clicking the Export Results button. The report gets downloaded to your browser.

You can click on the Endpoint Details link to see more authentication, accounting, and profiler information for a particular endpoint. The following figure shows an example of endpoint details information displayed for an endpoint.
Session Removal from the Directory

Sessions are cleaned from the session directory on the Monitoring and Troubleshooting node as follows:

- Terminated sessions are cleaned 15 minutes after termination.
- If there is authentication but no accounting, then such sessions are cleared after one hour.
- All inactive sessions are cleared after five days.

Related Topics

Global Search for Endpoints, on page 882

Authentication Summary Report

You can troubleshoot network access for a specific user, device, or search criteria based on attributes that are related to the authentication requests. You do this by running an Authentication Summary report.
Troubleshoot Network Access Issues

Step 1 Choose Operations > Reports > Authentication Summary Report.
Step 2 Filter the report for Failure Reasons.
Step 3 Review the data in the Authentication by Failure Reasons section of the report to troubleshoot your network access problem.

Note As the Authentication Summary report collects and displays the latest data corresponding to failed or passed authentications, the contents of the report appear after a delay of a few minutes.

Related Topics
Troubleshoot Unexpected RADIUS Authentication Results, on page 887

Diagnostic Troubleshooting Tools

Diagnostic tools help you diagnose and troubleshoot problems on a Cisco ISE network and provide a detailed instructions on how to resolve problems. You can use these tools to troubleshoot authentications and evaluate the configuration of any network device on your network, including Trustsec devices.

RADIUS Authentication Troubleshooting Tool

This tool allows you to search and select a RADIUS authentication or an Active Directory related RADIUS authentication for troubleshooting when there is an unexpected authentication result. You might use this tool if you expected an authentication to pass, but it failed or if you expected a user or machine to have a certain level of privileges, and the user or machine did not have those privileges.

• Searching RADIUS authentications based on Username, Endpoint ID, Network Access Service (NAS) IP address, and reasons for authentication failure for troubleshooting, Cisco ISE displays authentications only for the system (current) date.

• Searching RADIUS authentications based on NAS Port for troubleshooting, Cisco ISE displays all NAS Port values since the beginning of the previous month to the current date.

Note When searching RADIUS authentications based on NAS IP address and Endpoint ID fields, a search is first performed in the operational database, and then in the configuration database.

Troubleshoot Unexpected RADIUS Authentication Results

Step 1 Choose Operations > Troubleshoot > Diagnostic Tools > General Tools > RADIUS Authentication Troubleshooting.
Step 2 Specify the search criteria in the fields as needed.
Step 3  
Click Search to display the RADIUS authentications that match your search criteria.  
If you are searching for AD related authentication, and an Active Directory server is not configured in your deployment, a message saying 'AD not configured' is displayed.

Step 4  
Select a RADIUS authentication record from the table, and click Troubleshoot.  
If you need to troubleshoot AD related authentication, go to the Diagnostics Tool under Administration > Identity Management > External Identity Sources > Active Directory > AD node.

Step 5  
Click User Input Required, modify the fields as needed, and then click Submit.

Step 6  
Click Done.

Step 7  
Click Show Results Summary after the troubleshooting is complete.

Step 8  
To view a diagnosis, the steps to resolve the problem, and a troubleshooting summary, click Done.

---

**Execute Network Device Tool**

The Execute Network Device Command diagnostic tool allows you to run the *show* command on any network device. The results are exactly what you would see on a console, and can be used to identify problems in the configuration of the device. You can use it when you suspect that the configuration is wrong, you want to validate it, or if you are just curious about how it is configured.

**Execute IOS Show Commands to Check Configuration**

**Step 1**  

**Step 2**  
Enter the information in the appropriate fields.

**Step 3**  
Click Run to execute the command on the specified network device.

**Step 4**  
Click User Input Required, and modify the fields as necessary.

**Step 5**  
Click Submit to run the command on the network device, and view the output.

---

**Evaluate Configuration Validator Tool**

You can use this diagnostic tool to evaluate the configuration of a network device and identify any configuration problems. The Expert Troubleshooter compares the configuration of the device with the standard configuration.

**Troubleshoot Network Device Configuration Issues**

**Step 1**  
Choose Operations > Troubleshoot > Diagnostic Tools > General Tools > Evaluate Configuration Validator.

**Step 2**  
Enter the Network Device IP address of the device whose configuration you want to evaluate, and specify other fields as necessary.

**Step 3**  
Select the configuration options to compare against the recommended template.

**Step 4**  
Click Run.
Step 5  Click User Input Required, and modify the fields as necessary.
Step 6  Check the check boxes next to the interfaces that you want to analyze, and click Submit.
Step 7  Click Show Results Summary.

---

**Posture Troubleshooting Tool**

The Posture Troubleshooting tool helps you find the cause of a posture-check failure to identify the following:

- Which endpoints were successful in posture and which were not.
- If an endpoint failed in posture, what steps failed in the posture process.
- Which mandatory and optional checks passed and failed.

You determine this information by filtering requests based on parameters, such as username, MAC address, and posture status.

**Troubleshoot Endpoint Posture Failure**

- Enter the information in the appropriate fields.
- Click Search.
- To find an explanation and determine a resolution for an event, select the event in the list and click Troubleshoot.

**Session Trace Test Cases**

This tool allows you to test the policy flow in a predictable way to check and verify the way that the policy is configured, without needing to have real traffic originate from a real device.

You can configure the list of attributes and their values to be used in the Test Case. These details are used to perform interactions with the Policy system to simulate the runtime invocation of policy.

The attributes can be configured by using the dictionaries. All the dictionaries that are applicable to Simple RADIUS authentication are listed in the Attributes field.

**Note**

You can configure the Test Cases only for Simple RADIUS authentication.

**Configure Session Trace Test Case**

Before you begin

To perform the following task, you must be a Super Admin or System Admin.
Step 1 Choose Operations > Troubleshoot > Diagnostic Tools > General Tools > Session Trace Test Cases.

Step 2 Click Add.

Step 3 In the Test Details tab, enter a name and description for the Test Case.

Step 4 Select one of the predefined Test Cases or configure the required attributes and their values. The following predefined Test Cases are available:

- Basic Authenticated Access
- Profiled Cisco Phones
- Compliant Devices Access
- Wi-Fi Guest (Redirect)
- Wi-Fi Guest (Access)

When you select a predefined Test Case, Cisco ISE automatically populates the relevant attributes for the Test Case. You can use the default values for these attributes or select the desired value from the displayed options. You can also add additional custom attributes to the Test Case.

The attributes and the values that you add to the Test Case are listed in the Text field (below the Custom Attributes field). When you edit the content in the Text field, Cisco ISE checks the validity and syntax of the updated content.

You can view the summary of all the attributes at the bottom of the Test Details page.

Step 5 Click Submit to create a Test Case.

Cisco ISE validates the attributes and their values and indicates any errors before saving the test details.

Step 6 In the Test Visualizer tab, select the node on which you want to run this Test Case.

Only the nodes with Policy Service persona are displayed in the ISE Node drop-down list.

Click User Groups/Attributes to retrieve the groups and attributes for a user from an external identity store.

Step 7 Click Execute.

Cisco ISE executes the Test Case and displays the step-by-step results of the Test Case in a tabular format. It displays the policy stages, matching rules, and result objects. Click the green icon to view the details for each step.

Step 8 Click the Previous Test Executions tab to view the results of previous test executions. You can also select and compare any two Test Cases. Cisco ISE displays the comparative view of the attributes for each Test Case in a tabular format.

You can launch the Session Trace Test Case tool from the RADIUS Live Logs page. You can select an entry on the Live Logs page and click the Actions icon (on the Details column) to launch the Session Trace Test Case tool. Cisco ISE extracts the relevant attributes and their values from the corresponding log entry. You can modify these attributes and values, if required, and execute the Test Case.

**Technical Support Tunnel for Advanced Troubleshooting**

Cisco ISE uses the Cisco IronPort Tunnel infrastructure to create a secure tunnel for Cisco technical support engineers to connect to an ISE server and troubleshoot issues with the system. Cisco ISE uses SSH to create the secure connection through the tunnel.
As an administrator, you can control the tunnel access; you can choose when and how long to grant access to the support engineer. Cisco Customer Support cannot establish the tunnel without your intervention. You will receive notifications about the service logins. You can disable the tunnel connection at any point of time. By default, the technical support tunnel remains open for 72 hours; however, we recommend that you or the support engineer close the tunnel when all troubleshooting work is complete. You can choose to extend the tunnel beyond 72 hours, if needed.

You can use the `tech support-tunnel enable` command to initiate a tunnel connection.

The `tech support-tunnel status` command displays the status of the connection. This command provides information on whether the connection is established or not, or if there is an authentication failure, or if the servers are unreachable. If the tunnel server is reachable, but ISE is unable to authenticate, ISE tries to authenticate again every 5 minutes for a period of 30 minutes, after which the tunnel is disabled.

You can disable the tunnel connection using the `tech support-tunnel disable` command. This command disconnects an existing tunnel even if a support engineer is currently logged in.

If you have already established a tunnel connection from an ISE server, the SSH keys that are generated are available on the ISE server. When you try to enable the support tunnel at a later point of time, the system prompts you about reusing the SSH keys that were generated earlier. You can choose to use the same keys or generate new keys. You can also manually reset the keys using the `tech support-tunnel resetkey` command. If you execute this command when a tunnel connection is enabled, the system prompts you to disable the connection first. If you choose to continue with the existing connection and not disable it, the keys are reset after the existing connection is disabled. If you choose to disable the connection, the tunnel connection is dropped and the keys are reset immediately.

After you establish a tunnel connection, you can extend it using the `tech support-tunnel extend` command.

See the Cisco Identity Services Engine CLI Reference Guide for usage guidelines of the `tech support-tunnel` command.

### Establish a Technical Support Tunnel

You can establish a secure tunnel through the Cisco ISE Command Line Interface (CLI).

**Step 1**  
Enter the following command from the Cisco ISE CLI:  

```
tech support-tunnel enable
```

The system prompts you for a password and a nickname for the tunnel.

**Step 2**  
Enter the password.

**Step 3**  
(Optional) Enter a nickname for the tunnel.

The system generates an SSH key and displays the password, device serial number, and the SSH key. You must pass this information to Cisco Customer Support for the support engineer to connect to your system.

**Step 4**  
Copy the password, device serial number, and SSH key and send it to Cisco Customer Support.

The support engineer can now securely connect to your ISE server. You will receive periodic notifications about service logins.
TCP Dump Utility to Validate the Incoming Traffic

This is a tool to sniff the packet, when you want to examine that the expected packet really reached a node. For example, when there is no incoming authentication or log indicated in the report, you may suspect that there is no incoming traffic or that the incoming traffic cannot reach Cisco ISE. In such cases, you can run this tool to validate.

You can configure the TCP Dump options and then collect data from the network traffic to help you troubleshooting a network issue.

Caution

Starting a TCP Dump automatically deletes a previous dump file. To save a previous dump file, perform the task, as described in the Saving a TCP Dump File section before you begin a new TCP Dump session.

Related Topics

Save a TCP Dump File, on page 893

Use TCP Dump to Monitor Network Traffic

Before you begin

• The Network Interface drop-down list in the TCP Dump page displays only the network interface cards (NICs) that have an IPv4 or IPv6 address configured. By default, all NICs are connected on a VMware, and therefore, NICs are configured with an IPv6 address and displayed in the Network Interface drop-down list.

Step 1  Choose Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump.

Step 2  Choose a Host Name as the source for the TCP Dump utility.

Step 3  Choose a Network Interface to monitor from the drop-down list.

Step 4  Set Promiscuous Mode by clicking the radio button to On or Off. The default is On.

Promiscuous mode is the default packet sniffing mode in which the network interface passes all traffic to the system’s CPU. We recommend that you leave it set to On.

Step 5  In the Filter text box, enter a boolean expression on which to filter.

Supported standard tcpdump filter expressions:

  ip host 10.77.122.123
  ip host 10.77.122.123 and not 10.77.122.119
  ip host ISE123

Step 6  Click Start to begin monitoring the network.

Step 7  Click Stop when you have collected a sufficient amount of data, or wait for the process to conclude automatically after accumulating the maximum number of packets which is 500,000.
Cisco ISE does not support frames greater than 1500 MTU (jumbo frames).

Note
Cisco ISE does not support frames greater than 1500 MTU (jumbo frames).

Related Topics
Save a TCP Dump File, on page 893

Save a TCP Dump File

Before you begin
You should have successfully completed the task, as described in the Using TCP Dump to Monitor network Traffic section.

Note
You can also access TCPdump through the Cisco ISE CLI. For more information, refer to the Cisco Identity Services Engine CLI Reference Guide.

Step 1
Choose Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump.

Step 2
Choose a Format from the drop-down list. Human Readable is the default.

Step 3
Click Download, navigate to the desired location, and then click Save.

Step 4
To get rid of the previous dump file without saving it first, click Delete.

Compare Unexpected SGACL for an Endpoint or User

Step 1
Choose Operations > Troubleshoot > Diagnostic Tools > Trustsec Tools > Egress (SGACL) Policy.

Step 2
Enter the Network Device IP address of the Trustsec device whose SGACL policy you want to compare.

Step 3
Click Run.

Step 4
Click User Input Required and modify the fields as necessary.

Step 5
Click Submit.

Step 6
Click Show Results Summary to view the diagnosis and suggested resolution steps.

Egress Policy Diagnostic Flow

The egress policy diagnostic tool uses the process described in the following table for its comparison:
Troubleshoot Connectivity Issues in a Trustsec-Enabled Network with SXP-IP Mappings

<table>
<thead>
<tr>
<th>Process Stage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Connects to the device with the IP address that you provided, and obtains the access control lists (ACLs) for each source and destination SGT pair.</td>
</tr>
<tr>
<td>2</td>
<td>Checks the egress policy that is configured in Cisco ISE and obtains the ACLs for each source and destination SGT pair.</td>
</tr>
<tr>
<td>3</td>
<td>Compares the SGACL policy that is obtained from the network device with the SGACL policy that is obtained from Cisco ISE.</td>
</tr>
<tr>
<td>4</td>
<td>Displays the source and destination SGT pair if there is a mismatch. Also, displays the matching entries as additional information.</td>
</tr>
</tbody>
</table>

**Troubleshoot Connectivity Issues in a Trustsec-Enabled Network with SXP-IP Mappings**

**Step 1**  Choose **Operations > Troubleshoot > Diagnostic Tools > Trustsec Tools > SXP-IP Mappings**.

**Step 2**  Enter the network device IP address of the network device, and click **Select**.

**Step 3**  Click **Run**, and then click **User Input Required** and modify the necessary fields.

The Expert Troubleshooter retrieves Trustsec SXP connections from the network device and again prompts you to select the peer SXP devices.

**Step 4**  Click **User Input Required**, and enter the necessary information.

**Step 5**  Check the check box of the peer SXP devices for which you want to compare SXP mappings, and enter the common connection parameters.

**Step 6**  Click **Submit**.

**Step 7**  Click **Show Results Summary** to view the diagnosis and resolution steps.

**Troubleshoot Connectivity Issues in a Trustsec-Enabled Network with IP-SGT Mappings**

**Step 1**  Choose **Operations > Troubleshoot > Diagnostic Tools > Trustsec Tools > IP User SGT**.

**Step 2**  Enter the information in the fields as needed.

**Step 3**  Click **Run**.

You are prompted for additional input.

**Step 4**  Click **User Input Required**, modify the fields as necessary, and then click **Submit**.
Device SGT Tool

For devices that are enabled with the Trustsec solution, each network device is assigned an SGT value through RADIUS authentication. The Device SGT diagnostic tool connects to the network device (with the IP address that you provide) and obtains the network device SGT value. It then checks the RADIUS authentication records to determine the SGT value that was assigned most recently. Finally, it displays the Device-SGT pairs in a tabular format, and identifies whether the SGT values are the same or different.

Troubleshoot Connectivity Issues in a Trustsec-Enabled Network by Comparing Device SGT Mappings

Step 1 Choose Operations > Troubleshoot > Diagnostic Tools > Trustsec Tools > Device SGT.
Step 2 Enter the information in the fields as needed.
   The default port number for Telnet is 23 and SSH is 22.
Step 3 Click Run.
Step 4 Click Show Results Summary to view the results of the device SGT comparison.

Download Endpoint Statistical Data From Monitoring Nodes

You can download statistical data about endpoints that connect to your network from the Monitoring nodes. Key Performance Metrics (KPM), which include the load, CPU usage, authentication traffic data are available that you can use to monitor and troubleshoot issues in your network. From the Cisco ISE Command-Line Interface (CLI), use the application configure ise command and choose options 12 or 13 to download the daily KPM statistics or KPM statistics for the last eight weeks, respectively.

The output of this command provides the following data about endpoints:

• Total endpoints on your network
• Number of endpoints that established a successful connection
• Number of endpoints that failed authentication
• Total number of new endpoints that have connected each day
• Total number of endpoints onboarded each day

The output also includes time stamp details, the total number of endpoints that connected through each of the Policy Service Nodes (PSNs) in the deployment, total number of endpoints, active endpoints, load, and authentication traffic details.

Refer to the Cisco Identity Services Engine CLI Reference Guide for more information on this command.
Obtaining Additional Troubleshooting Information

Cisco ISE allows you to download support and troubleshooting information from the Admin portal. You can use the support bundle to prepare diagnostic information for the Cisco Technical Assistance Center (TAC) to troubleshoot problems with Cisco ISE.

The support bundles and debug logs provide advanced troubleshooting information for TAC and are difficult to interpret. You can use the various reports and troubleshooting tools that Cisco ISE provides to diagnose and troubleshoot issues that you are facing in your network.

Related Topics

Troubleshoot Network Access Issues, on page 887

Cisco ISE Support Bundle

You can configure the logs that you want to be part of your support bundle. For example, you can configure logs from a particular service to be part of your debug logs. You can also filter the logs based on dates.

The logs that you can download are categorized as follows:

- Full configuration database—The Cisco ISE configuration database is downloaded in a human-readable XML format. When you are trying to troubleshoot issues, you can import this database configuration in another Cisco ISE node to recreate the scenario.

- Debug logs—Captures bootstrap, application configuration, run-time, deployment, public key infrastructure (PKI) information and monitoring and reporting.

  Debug logs provide troubleshooting information for specific Cisco ISE components. To enable debug logs, see Chapter 11, “Logging”. If you do not enable the debug logs, all the informational messages (INFO) will be included in the support bundle. For more information, see Cisco ISE Debug Logs, on page 898.

- Local logs—Contains syslog messages from the various processes that run on Cisco ISE.

- Core files—Contains critical information that would help identify the cause of a crash. These logs are created when the application crashes and includes heap dumps.

- Monitoring and reporting logs—Contains information about alerts and reports.

- System logs—Contains Cisco Application Deployment Engine (ADE)-related information.

- Policy configuration—Contains policies configured in Cisco ISE in human readable format.

You can download these logs from the Cisco ISE CLI by using the backup-logs command. For more information, refer to the Cisco Identity Services Engine CLI Reference Guide.

Note

For Inline Posture nodes, you cannot download the support bundle from the Admin portal. You must use the backup-logs command from the Cisco ISE CLI to download logs for Inline Posture nodes.
If you choose to download these logs from the Admin portal, you can do the following:

- Download only a subset of logs based on the log type such as debug logs or system logs.
- Download only the latest “n” number of files for the selected log type. This option allows you to control the size of the support bundle and the time taken for download.

Monitoring logs provide information about the monitoring, reporting, and troubleshooting features. For more information about downloading logs, see Download Cisco ISE Log Files, on page 897.

Support Bundle

You can download the support bundle to your local computer as a simple tar.gpg file. The support bundle will be named with the date and time stamps in the format ise-support-bundle_ise-support-bundle-mm-dd-yyyy--hh-mm.tar.gpg. The browser prompts you to save the support bundle to an appropriate location. You can extract the content of the support bundle and view the README.TXT file, which describes the contents of the support bundle, as well as how to import the contents of the ISE database if it is included in the support bundle.

Download Cisco ISE Log Files

You can download the Cisco ISE log files to look for more information while troubleshooting issues in your network.

You can also download system logs that includes ADE-OS and other log files to troubleshoot installation and upgrade issues.

While downloading support bundle, instead of entering an encryption key manually, you can now choose to use a public key for encryption. If you choose this option, Cisco PKI will be used for encryption and decryption of the support bundle. Cisco TAC maintains the public and private keys. Cisco ISE uses the public keys to encrypt the support bundle. Cisco TAC can decrypt the support bundle using the private keys. Use this option if you want to provide the support bundle to Cisco TAC for troubleshooting. Use the shared key encryption if you are going to troubleshoot the issues on premise.

Before you begin

- You must have Super Admin or System Admin privileges to perform the following task.
- Configure debug logs and the debug log levels.

Step 1 Choose Operations > Troubleshoot > Download Logs > Appliance node list.
Step 2 Click the node from which you want to download the support bundles.
Step 3 In the Support Bundle tab, choose the parameters that you want to be populated in your support bundle.

If you include all the logs, your support bundle will be excessively large and the download will take a long time. To optimize the download process, choose to download only the most recent n number of files.

Step 4 Enter the From and To dates for which you want to generate the support bundle.
Step 5 Choose one of the following:

- Public Key Encryption—Choose this option if you want to provide the support bundle to Cisco TAC for troubleshooting purposes.
• Shared Key Encryption—Choose this option if you want to troubleshoot the issues locally on premise. If you choose this option, you must enter the encryption key for the support bundle.

**Step 6** Enter and re-enter the encryption key for the support bundle.

**Step 7** Click **Create Support Bundle**.

**Step 8** Click **Download** to download the newly-created support bundle.

The support bundle is a tar.gpg file that is downloaded to the client system that is running your application browser.

---

**What to do next**

Download debug Logs for specific components.

**Related Topics**

[Download Debug Logs](#), on page 900

---

**Cisco ISE Debug Logs**

Debug logs provide troubleshooting information for various Cisco ISE components. Debug logs contain critical and warning alarms generated in the last 30 days and info alarms generated in the last 7 days. While reporting problems, you might be asked to enable these debug logs and send them for diagnosis and resolution of your problems.

**Obtain Debug Logs**

**Step 1** Configure the components for which you want to obtain the debug logs on the Debug Log Configuration page.

**Step 2** Download the debug logs.

**Related Topics**

[Download Debug Logs](#), on page 900

---

**Cisco ISE Components and the Corresponding Debug Logs**

**Table 71: Components and Corresponding Debug Logs**

<table>
<thead>
<tr>
<th>Component</th>
<th>Debug Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>ad_agent.log</td>
</tr>
<tr>
<td>Cache Tracker</td>
<td>tracking.log</td>
</tr>
<tr>
<td>Entity Definition Framework (EDF)</td>
<td>edf.log</td>
</tr>
<tr>
<td>JMS</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>License</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>Notification Tracker</td>
<td>tracking.log</td>
</tr>
<tr>
<td>Replication-Deployment</td>
<td>replication.log</td>
</tr>
</tbody>
</table>
## Cisco ISE Components and the Corresponding Debug Logs

<table>
<thead>
<tr>
<th>Component</th>
<th>Debug Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replication-JGroup</td>
<td>replication.log</td>
</tr>
<tr>
<td>Replication Tracker</td>
<td>tracking.log</td>
</tr>
<tr>
<td>RuleEngine-Attributes</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>RuleEngine-Policy-IDGroups</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>accessfilter</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>admin-infra</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>boot-strap wizard</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>cisco-mnt</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>client</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>cpm-clustering</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>cpm-mnt</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>epm-pdp</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>epm-pip</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>anc</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>anc</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>ers</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>guest</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>Guest Access Admin</td>
<td>guest.log</td>
</tr>
<tr>
<td>Guest Access</td>
<td>guest.log</td>
</tr>
<tr>
<td>MyDevices</td>
<td>guest.log</td>
</tr>
<tr>
<td>Portal</td>
<td>guest.log</td>
</tr>
<tr>
<td>Portal-Session-Manager</td>
<td>guest.log</td>
</tr>
<tr>
<td>Portal-web-action</td>
<td>guest.log</td>
</tr>
<tr>
<td>guestauth</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>guestportal</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>identitystore-AD</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>infrastructure</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>mdm</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>mdm-pip</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>mnt-alarm</td>
<td>alarms.log</td>
</tr>
<tr>
<td>mnt-report</td>
<td>reports.log</td>
</tr>
</tbody>
</table>
### Debug Log Components

<table>
<thead>
<tr>
<th>Component</th>
<th>Debug Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>mydevices</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>nsf</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>nsf-session</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>org-apache</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>org-apache-cxf</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>org-apache-digester</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>posture</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>profiler</td>
<td>profiler.log</td>
</tr>
<tr>
<td>provisioning</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>prrt-JNI</td>
<td>prrt-management.log</td>
</tr>
<tr>
<td>runtime-AAA</td>
<td>prrt-management.log</td>
</tr>
<tr>
<td>runtime-config</td>
<td>prrt-management.log</td>
</tr>
<tr>
<td>runtime-logging</td>
<td>prrt-management.log</td>
</tr>
<tr>
<td>sponsorportal</td>
<td>ise-psc.log</td>
</tr>
<tr>
<td>swiss</td>
<td>ise-psc.log</td>
</tr>
</tbody>
</table>

### Download Debug Logs

**Before you begin**

To perform the following task, you must be a Super Admin or System Admin.

**Step 1** Choose **Operations > Troubleshoot > Download Logs > Appliance node list.**

**Step 2** From the Appliance node list, click the node from which you want to download the debug logs.

**Step 3** Click the **Debug Logs** tab.

A list of debug log types and debug logs is displayed. This list is based on your debug log configuration.

**Step 4** Click the log file that you want to download and save it to the system that is running your client browser.

You can repeat this process to download other log files as needed. The following are additional debug logs that you can download from the Debug Logs page:

- **isebootstrap.log**—Provides bootstrapping log messages
- **monit.log**—Provides watchdog messages
- **pki.log**—Provides the third-party crypto library logs
- **iseLocalStore.log**—Provides logs about the local store files
- **ad_agent.log**—Provides Microsoft Active Directory third-party library logs
Monitoring Database

The rate and amount of data that is utilized by Monitoring functions requires a separate database on a dedicated node that is used for these purposes.

Like Policy Service, Monitoring has a dedicated database that requires you to perform maintenance tasks, such as the topics covered in this section:

Related Topics
- Log Collection, on page 880
- Back Up and Restore of the Monitoring Database, on page 901
- Monitoring Database Purge, on page 901

Back Up and Restore of the Monitoring Database

Monitoring database handles large volumes of data. Over time, the performance and efficiency of the monitoring node depends on how well you manage that data. To increase efficiency, we recommend that you back up the data and transfer it to a remote repository on a regular basis. You can automate this task by scheduling automatic backups.

Note
You should not perform a backup when a purge operation is in progress. If you start a backup during a purge operation, the purge operation stops or fails.

If you register a secondary Monitoring node, we recommend that you first back up the primary Monitoring node and then restore the data to the new secondary Monitoring node. This ensures that the history of the primary Monitoring node is in sync with the new secondary node as new changes are replicated.

Monitoring Database Purge

The purging process allows you to manage the size of the Monitoring database by specifying the number of months to retain data during a purge. The default is three months. This value is utilized when the disk space usage threshold for purging (percentage of disk space) is met. For this option, each month consists of 30 days. A default of three months equals 90 days.

Related Topics
- Guidelines for Purging the Monitoring Database, on page 901

Guidelines for Purging the Monitoring Database

The following are some guidelines to follow relating to Monitoring database disk usage:
• If the Monitoring database disk usage is greater than 80 percent of the threshold setting, critical alarm is generated indicating that the database size has exceeded the allocated disk size. If the disk usage is greater than 90 percent another alarm is generated.

A purge process runs, creating a status history report that you can view by choosing Operations > Reports > Deployment Status > Data Purging Audit. An information (INFO) alarm is generated when the purge completes.

• Purging is also based on the percentage of consumed disk space for the database. When the consumed disk space for the Monitoring database is equal to or exceeds the threshold (the default is 80 percent), the purge process starts. This process deletes only the last seven days of monitoring data, irrespective of what is configured in the Admin portal. It will continue this process in a loop until the disk space is below 80 percent. Purging always checks the Monitoring database disk space limit before proceeding.

Operational Data Purging

ISE MnT Operational (OPS) database contains information that is generated as ISE reports. Recent ISE releases have options to Purge M&T Operational Data and Reset M&T Database after running the ISE admin CLI command application configure ise.

The purge option is used to clean up the data and will prompt to ask the number of days to be retained. The reset option is used to reset the database to the factory default, so that all the data that is backed up will be permanently deleted. You can reset the database if the files are consuming too much file system space.

Note

The reset option will cause ISE services to be temporarily unavailable until it restarts.

The Operational Data Purging page (Administration > System > Maintenance > Operational Data Purging) contains the Database Utilization and Purge Data Now areas. You can view the total available database space and the RADIUS and TACACS data stored in the Database Utilization area. You can hover the mouse over the status bar to display the available disk space and the number of days the existing data is stored in the database. You can specify the period during which the RADIUS and TACACS data is supposed to be retained in the Data Retention Period area. Data is purged at 4 a.m. every day, and you can configure to export data to a repository before it is purged by specifying the number of retention days. You can check the Enable Export Repository check box to select and create a repository, and specify an Encryption Key.

In the Purge Data Now area, you can purge all RADIUS and TACACS data or specify the number of days beyond which data is supposed to be purged.

Note

You can export the RADIUS authentication and accounting, TACACS authorization and accounting, RADIUS errors, and Misconfigured supplicants tables to a repository before purging.

Related Topics

Purge Older Operational Data, on page 902

Purge Older Operational Data

The operational data gets collected in the server over a period of time. It can be purged either instantly or periodically. You can verify the success of the data purge by viewing the Data Purging Audit report.
Before you begin

To perform the following task, you must be a Super Admin or System Admin.

---

**Step 1**  
Choose **Administration > System > Maintenance > Operational Data Purging**.

**Step 2**  
Do one of the following:

- In the Data Retention Period area:
  1. Specify the time period in days, for which RADIUS and TACACS data should be retained. All the data prior to the specified time period will be exported to a repository.
  2. In the Repository area, check the Enable Export Repository check box to choose the repository to save data. Refer to the Create Repositories section for more information.
  3. In the Encryption Key text box, enter the required password.
  4. Click Save.

**Note**  
If the configured retention period is less than the existing retention thresholds corresponding to the diagnostics data, then the configured value overrides the existing threshold values. For example, if you configure the retention period as 3 days and this value is less than the existing thresholds in the diagnostics tables (for example, a default of 5 days), then data is purged according to the value that you configure (3 days) in this page.

- In the Purge Data Now area:
  1. Choose to purge all data or to purge data that is older than the specified number of days. Data is not saved in any repository.
  2. Click Purge.

---

**Database Crash/File Corruption Issues**

Cisco ISE may crash if the oracle database files are corrupted due to power outage or other reasons resulting in data loss. Based on the incident, follow the steps below to recover from data loss.

- In case of PAN corruption in deployment, you should **promote the Secondary PAN to Primary PAN**.
- If SPAN is promotion is not possible due to small deployment or any other reason, **restore** the most recent available backup.
- In case of PSN corruption, follow the steps to **de-register, reset config and register** the node again.
- In case of Standalone box, **restore** most recent available backup.

**Note**  
Obtain backup from the standalone box regularly to avoid loss in the latest configuration changes.
Cisco ISE Reports

Cisco Identity Services Engine (ISE) reports are used with monitoring and troubleshooting features to analyze trends, and, monitor system performance and network activities from a central location.

Cisco ISE collects log and configuration data from across the network. It then aggregates the data into reports for you to view and analyze. Cisco ISE provides a standard set of predefined reports that you can use and customize to fit your needs.

Cisco ISE reports are preconfigured and e grouped into logical categories with information related to authentication, session traffic, device administration, configuration and administration, and troubleshooting.

Related Topics
- Run and View Reports, on page 907
- Export Reports, on page 908
- Available Reports, on page 911

Report Filters

There are two types of reports, single-section and multi-section. Single-section reports contain a single grid (Radius Authentications report) and multi-section reports contain many grids (Authentications Summary report) and represent data in the form of charts and tables. The Filter drop-down menu in the single-section reports contains the Quick Filter and Advanced Filter. In the multi-section reports, you can specify only advanced filters.
Multi-section reports may contain one or more mandatory advanced filters that require your input. For example, when you click the Health Summary report (Operations > Reports > Diagnostics page), it displays two mandatory advanced filters—Server and Time Range. You must specify the operator command, server name, required values for both these filters, and click Go to generate the report. You can add new advanced filters by clicking the Plus (+) symbol. You can export multi-section reports only in the PDF format. You cannot schedule Cisco ISE multi-section reports to run and re-run at specific time or time intervals.

---

**Note**

When you click a report, data for the current date is generated by default. However, some multi-section reports require mandatory input from the user apart from the time range.

By default, the Quick Filter is displayed as the first row in single-section reports. The fields may contain a drop-down list from which you can select the search criteria or may be a text box.

An Advanced Filter contains an outer criteria that contains one or more inner criteria. The outer criteria is used to specify if the search should meet All or Any specified inner criteria. The inner criteria contains one or more conditions that is used to specify the Category (Endpoint ID, Identity Group) Method (operator commands, such as Contains, Does Not Contain), and Time Range for the condition.

When using the Quick Filter, you can choose a date or time from the Logged At drop-down list to generate reports for a data set logged in the last 30 days or less. If you want to generate a report for a date or time prior to 30 days, use the Advanced Filter to set the required time frame in the From and To fields of the Custom option from the drop-down list.

---

**Create the Quick Filter Criteria**

The section describes how to create a quick filter criteria. You can create quick filter criteria for only single-section reports.

**Step 1** Choose Operations > Reports and click the required report.

**Step 2** From the Settings drop-down list, choose the required fields.

**Step 3** In the required field, you can choose from the drop-down list or type the specific characters to filter data. The search uses the Contains operator command. For example, to filter by text that begins with “K”, enter K or to filter text that has “geo” anywhere in the text, enter geo. You can also use asterisks (*), for example, the regex starting with *abc and ending with *def.

The quick filter uses the following conditions: contains, starts with, ends with, starts with or ends with, and multiple values with OR operator.

**Step 4** Press Enter.

---

**Create the Advanced Filter Criteria**

The section describes how to create an advanced filter criteria. You can create advanced filters for single- and multi-section reports. The Filter drop-down menu in the single-section reports contains the Quick Filter and Advanced Filter. In the multi-section reports, you can specify only advanced filters.
Run and View Reports

This section describes how to run, view, and navigate reports using Reports View. When you click a report, by default, data for the last seven days is generated. You can specify time increments over which to display data in a report.

Step 1  Choose Operations > Reports > ISE Reports.
Step 2  You can also navigate to the Reports link under each work center to view the set of reports specific to that work center.
Step 3  Click a report from the report categories available.
Step 4  Select one or more filters to run a report. Each report has different filters available, of which some are mandatory and some are optional.
Step 5  Enter an appropriate value for the filters.
Step 6  Click Go.

You can save a filtered report and retrieve it from the Filter drop-down list for future reference.

Reports Navigation

You can get detailed information from the reports output. For example, if you have generated a report for a period of five months, the graph and table will list the aggregate data for the report in a scale of months.
You can click a particular value from the table to see another report related to this particular field. For example, an authentication summary report will display the failed count for the user or user group. When you click the failed count, an authentication summary report is opened for that particular failed count.

## Export Reports

You can export report data in the following file formats:

- Excel spreadsheet as a Comma Separated Values (.csv) file. After you export the data, you will receive an email detailing the location of the report.
- Microsoft Excel Comma Separated Values (.csv) file that can be saved to a local disk.
- Adobe Acrobat Document (.pdf) file that can be saved to a local disk.

---

**Note**

You can export 5000 records for Microsoft Excel and 1000 records for PDF file formats.

You can only export the PDF file format of the following reports:

- Authentication Summary
- Health Summary
- RBACL Drop Summary

---

**Note**

Flows for RBACL dropped packets are available only with the Cisco Catalyst 6500 series switches.

- Guest Sponsor summary
- End point Profile Changes
- Network Device Session Status

---

**Note**

To view the non-English characters correctly after exporting a report, you must import the file into Microsoft Excel by enabling UTF-8 character encoding. If you choose to open the exported .csv file directly in Microsoft Excel without enabling UTF-8 character encoding, the non-English characters in the report appear in some garbage form.

---

**Note**

You can export report data to a .csv format only from the Primary PAN.

---

**Step 1**

Run a report, as described in the Running and Viewing Reports section.
**Scheduling and Saving the Reports**

You can customize a report and save the changes as a new report, or restore the default report settings in My Reports at the top right corner of the report summary page.

You can also customize and schedule Cisco ISE reports to run and re-run at specific time or time intervals. You can also send and receive email notifications once the reports are generated.

---

**Note**

If a scheduled report is created by an external administrator (Eg: Active Directory Administrator) without filling in the email-id field, then there will be no email notification sent.

You cannot schedule the following reports:

- Authentication Summary
- Health Summary
- RBACL Drop Summary
- Guest Sponsor summary
- End point Profile Changes
- Network Device Session Status

---

**Note**

You can save or schedule (customize) Cisco ISE reports only from the PAN.

---

**Step 1**

Run a report as described in the Running and Viewing Reports section.

**Step 2**

Click My Reports in the top right-hand corner of the report summary page.

**Step 3**

Enter the required details in the dialog box.

**Step 4**

Click Save as New.

After saving a report, when you go back to the saved report all the filter options are checked by default. You need to uncheck the filters that you do not wish to use.

You can also remove the saved report from My Reports category.
Cisco ISE Active RADIUS Sessions

Cisco ISE provides a dynamic Change of Authorization (CoA) feature for the Live Sessions that allows you to dynamically control active RADIUS sessions. You can send reauthenticate or disconnect requests to a Network Access Device (NAD) to perform the following tasks:

- Troubleshoot issues related to authentication—You can use the Session reauthentication option to follow up with an attempt to reauthenticate again. However, you must not use this option to restrict access. To restrict access, use the shutdown option.

- Block a problematic host—You can use the Session termination with port shutdown option to block an infected host that sends a lot of traffic over the network. However, the RADIUS protocol does not currently support a method for re-enabling a port that has been shut down.

- Force endpoints to reacquire IP addresses—You can use the Session termination with port bounce option for endpoints that do not have a supplicant or client to generate a DHCP request after a VLAN change.

- Push an updated authorization policy to an endpoint—You can use the Session reauthentication option to enforce an updated policy configuration, such as a change in the authorization policy on existing sessions based on the discretion of the administrator. For example, if posture validation is enabled, when an endpoint gains access initially, it is usually quarantined. After the identity and posture of the endpoint are known, it is possible to send the Session reauthentication command to the endpoint for the endpoint to acquire the actual authorization policy based on its posture.

For CoA commands to be understood by the device, it is important that you configure the options appropriately.

For CoA to work properly, you must configure the shared secret of each device that requires a dynamic change of authorization. Cisco ISE uses the shared secret configuration to request access from the device and issue CoA commands to it.

Note

In this release of Cisco ISE, the maximum number of active authenticated endpoint sessions that can be displayed is limited to 100,000.

Related Topics

Change Authorization for RADIUS Sessions, on page 910

Change Authorization for RADIUS Sessions

Some Network Access Devices on your network may not send an Accounting Stop or Accounting Off packet after a reload. As a result, you might find two sessions in the Session Directory reports, one which has expired.

To dynamically change the authorization of an active RADIUS session or disconnect an active RADIUS session, be sure to choose the most recent session.

Step 1  Choose Operations > RADIUS Livelog.
Step 2  Switch the view to Show Live Session.
Step 3  Click the CoA link for the RADIUS session that you want to issue CoA and choose one of the following options:

- SAnet Session Query—Use this to query information about sessions from SAnet supported devices.
• **Session reauthentication**—Reauthenticate session. If you select this option for a session established on an ASA device supporting COA, this will invoke a Session Policy Push CoA.

• **Session reauthentication with last**—Use the last successful authentication method for this session.

• **Session reauthentication with rerun**—Run through the configured authentication method from the beginning.

  **Note**  
  *Session reauthentication with last* and *Session reauthentication with rerun* options are not currently supported in Cisco IOS software.

• **Session termination**—Just end the session. The switch reauthenticates the client in a different session.

• **Session termination with port bounce**—Terminate the session and restart the port.

• **Session termination with port shutdown**—Terminate the session and shutdown the port.

**Step 4**  
Click **Run** to issue CoA with the selected reauthenticate or terminate option.

If your CoA fails, it could be one of the following reasons:

• Device does not support CoA.

• Changes have occurred to the identity or authorization policy.

• There is a shared secret mismatch.

---

**Available Reports**

The following table lists the preconfigured reports, grouped according to their category. Descriptions of the report functionality and logging category are also provided.
PART VII

Reference

- Administration User Interface Reference, on page 915
- Guest Access User Interface Reference, on page 1035
- Web Portals Customization Reference, on page 1065
- Policy User Interface Reference, on page 1079
- Operations User Interface Reference, on page 1153
- Network Access Flows, on page 1173
- Switch and Wireless LAN Controller Configuration Required to Support Cisco ISE Functions, on page 1181
- Supported Management Information Bases for Cisco ISE Endpoint Profiler, on page 1193
CHAPTER 30

Administration User Interface Reference

- Deployment and Node Settings, on page 915
- Identity Management, on page 970
- Network Resources, on page 988
- Device Portal Management, on page 1013

Deployment and Node Settings

Deployment Settings

The Deployment Nodes page enables you to configure Cisco ISE (Administration, Policy Service, and Monitoring) nodes and to set up a deployment.

Deployment Nodes List Page

The following table describes the fields on the Deployment Nodes List page, which you can use to configure Cisco ISE nodes in a deployment. The navigation path for this page is: Administration > System > Deployment.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Displays the hostname of the node.</td>
</tr>
<tr>
<td>Node Type</td>
<td>Displays the node type. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Cisco ISE (Administration, Policy Service, and Monitoring) nodes</td>
</tr>
<tr>
<td>Personas</td>
<td>(Only appears if the node type is Cisco ISE) Lists the personas that an Cisco ISE node has assumed. For example, Administration, Policy Service.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Role         | Indicates the role (primary, secondary, or standalone) that the Administration and Monitoring personas have assumed, if these personas are enabled on this node. The role can be any one or more of the following:  
- PRI(A)—Refers to the Primary PAN  
- SEC(A)—Refers to the Secondary PAN  
- PRI(M)—Refers to the Primary Monitoring Node  
- SEC(M)—Refers to the Secondary Monitoring Node |
| Services     | (Only appears if the Policy Service persona is enabled) Lists the services that run on this Cisco ISE node. Services can include any one of the following:  
- Session  
- Profiling  
- All |
| Node Status  | Indicates the status of each ISE node in a deployment for data replication.  
- Green (Connected)—Indicates that an ISE node, which is already registered in the deployment is in sync with the Primary PAN.  
- Red (Disconnected)—Indicates that an ISE node is not reachable or is down or data replication is not happening.  
- Orange (In Progress)—Indicates that an ISE node is newly registered with the Primary PAN or you have performed a manual sync operation or the ISE node is not in sync (out of sync) with the Primary PAN.  
For more details, click the quick view icon for each ISE node in the Node Status column. |

Related Topics
- Cisco ISE Distributed Deployment, on page 48
- Cisco ISE Deployment Terminology, on page 47
- Configure a Cisco ISE Node, on page 51
- Register a Secondary Cisco ISE Node
General Node Settings

The following table describes the fields on the General Node Settings page, which you can use to set up your deployment and configure services to be run on each of the nodes. The navigation path for this tab is: Administration > System > Deployment > ISE Node > Edit > General Settings.

Table 72: General Node Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Displays the hostname of the Cisco ISE node.</td>
</tr>
<tr>
<td>FQDN</td>
<td>Displays the fully qualified domain name of the Cisco ISE node. For example, ise1.cisco.com.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Displays the IP address of the Cisco ISE node.</td>
</tr>
<tr>
<td>Node Type</td>
<td>Displays the node type.</td>
</tr>
<tr>
<td>Personas</td>
<td>Check this check box if you want a Cisco ISE node to assume the Administration persona. You can enable the Administration persona only on nodes that are licensed to provide the administrative services. Role—Displays the role that the Administration persona has assumed in the deployment. Could take on any one of the following values: Standalone, Primary, Secondary Make Primary—Click this button to make this node your primary Cisco ISE node. You can have only one primary Cisco ISE node in a deployment. The other options on this page will become active only after you make this node primary. You can have only two Administration nodes in a deployment. If the node has a Standalone role, a Make Primary button appears next to it. If the node has a Secondary role, a Promote to Primary button appears next to it. If the node has a Primary role and there are no other nodes registered with it, a Make Standalone button appears next to it. You can click this button to make your primary node a standalone node.</td>
</tr>
</tbody>
</table>
### Fields

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
</table>
| Monitoring | Check this check box if you want a Cisco ISE node to assume the Monitoring persona and function as your log collector. There must be at least one Monitoring node in a distributed deployment. At the time of configuring your Primary PAN, you must enable the Monitoring persona. After you register a secondary Monitoring node in your deployment, you can edit the Primary PAN and disable the Monitoring persona, if required. To configure a Cisco ISE node on a VMware platform as your log collector, use the following guidelines to determine the minimum amount of disk space that you need: 180 KB per endpoint in your network, per day 2.5 MB per Cisco ISE node in your network, per day. You can calculate the maximum disk space that you need based on how many months of data you want to have in your Monitoring node. If there is only one Monitoring node in your deployment, it assumes the standalone role. If you have two Monitoring nodes in your deployment, Cisco ISE displays the name of the other monitoring node for you to configure the Primary-Secondary roles. To configure these roles, choose one of the following:

- **Primary**—For the current node to be the primary Monitoring node.
  
- **Secondary**—For the current node to be the secondary Monitoring node.
  
- **None**—If you do not want the Monitoring nodes to assume the primary-secondary roles.

If you configure one of your Monitoring nodes as primary or secondary, the other Monitoring node automatically becomes the secondary or primary node, respectively. Both the primary and secondary Monitoring nodes receive Administration and Policy Service logs. If you change the role for one Monitoring node to None, the role of the other Monitoring node also becomes None, thereby cancelling the high availability pair After you designate a node as a Monitoring node, you will find this node listed as a syslog target in the following page: Administration > System > Logging > Remote Logging Targets |
<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Service</td>
<td></td>
</tr>
</tbody>
</table>
Check this checkbox to enable any one or all of the following services:

- **Enable Session Services**—Check this checkbox to enable network access, posture, guest, and client provisioning services. Choose the group to which this Policy Service node belongs from the Include Node in Node Group drop-down list. Choose <none> if you do not want this Policy Service node to be part of any group.

All the nodes within the same node group should be configured on the network access device (NAD) as RADIUS clients and authorized for CoA, because any one of them can issue a CoA request for the sessions that are established through any node in the node group. If you are not using a load balancer, the nodes in a node group should be the same as, or a subset of the RADIUS servers and clients configured on the NAD. These nodes would also be configured as RADIUS servers.

While a single NAD can be configured with many ISE nodes as RADIUS servers and dynamic-authorization clients, it is not necessary for all the nodes to be in the same node group.

The members of a node group should be connected to each other using high-speed LAN connection such as Gigabit Ethernet. The node group members need not be L2 adjacent, but L2 adjacency is highly recommended to ensure sufficient bandwidth and reachability. See Create a Policy Service Node Group, on page 70 section for more details.

- **Enable Profiling Service**—Check this checkbox to enable the Profiler service. If you enable the Profiling service, you must click the Profiling Configuration tab and enter the details as required. When you enable or disable any of the services that run on the Policy Service node or make any changes to this node, you will be restarting the application server processes on which these services run. You must expect a delay while these services restart. You can determine when the application server has restarted on a node by using the show application status ise command from the CLI.

- **Enable Threat Centric NAC Service**—Check this
### Usage Guidelines

Check box to enable the Threat Centric Network Access Control (TC-NAC) feature. This feature allows you to create authorization policies based on the threat and vulnerability attributes received from the threat and vulnerability adapters. Threat severity levels and vulnerability assessment results can be used to dynamically control the access level of an endpoint or a user.

- **Enable SXP Service**—Check this check box to enable SXP service on the node. You must also specify the interface to be used for SXP service.
  
  If you have configured NIC bonding or teaming, the bonded interfaces are also listed along with the physical interfaces in the Use Interface drop-down list.

- **Enable Device Admin Service**—Check this check box to create TACACS policy sets, policy results, and so on to control and audit the configuration of network devices.

- **Enable Passive Identity Service**—Check this check box to enable the Identity Mapping feature. This feature enables you to monitor users that are authenticated by a Domain Controller (DC) and not by Cisco ISE. In networks where Cisco ISE does not actively authenticate users for network access, you can use the Identity Mapping feature to collect user authentication information from the Active Directory (AD) Domain Controller.

- **pxGrid**

  Check this check box to enable pxGrid persona. Cisco pxGrid is used to share the context-sensitive information from Cisco ISE session directory to other policy network systems such as Cisco Adaptive Security Appliance (ASA). The pxGrid framework can also be used to exchange policy and configuration data between nodes like sharing tags and policy objects between ISE and third party vendors, and for non-ISE related information exchanges such as threat information.

### Related Topics

- [Personas in Distributed Cisco ISE Deployments](#), on page 48
- [Administration Node](#), on page 54
- [Policy Service Node](#), on page 61
- [Monitoring Node](#), on page 62
Profiling Node Settings

The following table describes the fields on the Profiling Configuration page, which you can use to configure the probes for the profiler service. The navigation path for this page is: Administration > System > Deployment > ISE Node > Edit > Profiling Configuration.

### Table 73: Profiling Node Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
</table>
| NetFlow     | Check this check box if you want to enable NetFlow per Cisco ISE node that has assumed the Policy Service persona to receive Netflow packets sent from the routers. Choose these options:  
  • Interface—Choose the interface on the ISE node.  
  • Port—Enter the NetFlow listener port number on which NetFlow exports are received from the routers. The default port is 9996. |
| DHCP        | Check this check box if you want to enable DHCP per Cisco ISE node that has assumed the Policy Service persona to listen for DHCP packets from IP helper. Choose these options:  
  • Interface—Choose the interface on the ISE node.  
  • Port—Enter the DHCP server UDP port number. The default port is 67. |
| DHCP SPAN   | Check this check box if you want to enable DHCP SPAN per Cisco ISE node that has assumed the Policy Service persona to collect DHCP packets.  
  • Interface—Choose the interface on the ISE node. |
| HTTP        | Check this check box if you want to enable HTTP per Cisco ISE node that has assumed the Policy Service persona to receive and parse HTTP packets.  
  • Interface—Choose the interface on the ISE node. |
<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS</td>
<td>Check this check box if you want to enable RADIUS per ISE node that has assumed the Policy Service persona to collect RADIUS session attributes as well as CDP, LLDP attributes from the IOS Sensor enabled devices.</td>
</tr>
<tr>
<td>Network Scan (NMAP)</td>
<td>Check this box to enable the NMAP probe.</td>
</tr>
<tr>
<td>DNS</td>
<td>Check this check box if you want to enable DNS per ISE node that has assumed the Policy Service persona to perform a DNS lookup for the FQDN. Enter the timeout period in seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> For the DNS probe to work on a particular Cisco ISE node in a distributed deployment, you must enable any one of the following probes: DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP. For DNS lookup, one of the probes mentioned above must be started along with the DNS probe.</td>
</tr>
<tr>
<td>SNMP Query</td>
<td>Check this check box if you want to enable SNMP Query per ISE node that has assumed the Policy Service persona to poll network devices at specified intervals. Enter values for the following fields: Retries, Timeout, Event Timeout, and an optional Description.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> In addition to configuring the SNMP Query probe, you must also configure other SNMP settings in the following location: Administration &gt; Network Resources &gt; Network Devices. When you configure SNMP settings on the network devices, ensure that you enable the Cisco Device Protocol (CDP) and Link Layer Discovery Protocol (LLDP) globally on your network devices.</td>
</tr>
</tbody>
</table>
Fields | Usage Guidelines
---|---
SNMP Trap | Check this check box if you want to enable SNMP Trap probe per ISE node that has assumed the Policy Service Persona to receive linkUp, linkDown, and MAC notification traps from the network devices. Choose any of the following:
- Link Trap Query—Check this check box to receive and interpret linkup and linkdown notifications received through the SNMP Trap.
- MAC Trap Query—Check this check box to receive and interpret MAC notifications received through the SNMP Trap.
- Interface—Choose an interface on the ISE node.
- Port—Enter the UDP port of the host to use. The default port is 162.

Active Directory | Scans the defined Active Directory servers for information about Windows users.
pxGrid | Allows ISE to collect (profile) endpoint attributes over pxGrid.

Related Topics
- Cisco ISE Profiling Service, on page 643
- Network Probes Used by Profiling Service, on page 646
- Configure Profiling Service in Cisco ISE Nodes, on page 645

Certificate Store Settings

The Certificate Store page enables you to configure certificates in Cisco ISE that can be used for authentication.

Self-Signed Certificate Settings

The following table describes the fields in the Generate Self Signed Certificate page. This page allows you to create system certificates for inter-node communication, EAP-TLS authentication, Cisco ISE web portals, and to communicate with the pxGrid controller. The navigation path for this page is: Administration > System > Certificates > System Certificates > Generate Self Signed Certificate.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Node</td>
<td>(Required) The node for which you want to generate the system certificate.</td>
</tr>
<tr>
<td>Common Name (CN)</td>
<td>(Required if you do not specify a SAN) By default, the common name is the Fully Qualified Domain Name of the ISE node for which you are generating the self-signed certificate.</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>Organizational Unit name. For example, Engineering.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Organization name. For example, Cisco.</td>
</tr>
<tr>
<td>City (L)</td>
<td>(Do not abbreviate) City name. For example, San Jose.</td>
</tr>
<tr>
<td>State (ST)</td>
<td>(Do not abbreviate) State name. For example, California.</td>
</tr>
<tr>
<td>Country (C)</td>
<td>Country name. You must enter the two-letter ISO country code. For example, US.</td>
</tr>
<tr>
<td>Subject Alternative Name (SAN)</td>
<td>An IP address, DNS name, or Uniform Resource Identifier (URI) that is associated with the certificate.</td>
</tr>
<tr>
<td>Key Type</td>
<td>Specify the algorithm to be used for creating the public key: RSA or ECDSA.</td>
</tr>
<tr>
<td>Key Length</td>
<td>Specify the bit size for the public key.</td>
</tr>
<tr>
<td></td>
<td>The following options are available for RSA:</td>
</tr>
<tr>
<td></td>
<td>• 512</td>
</tr>
<tr>
<td></td>
<td>• 1024</td>
</tr>
<tr>
<td></td>
<td>• 2048</td>
</tr>
<tr>
<td></td>
<td>• 4096</td>
</tr>
<tr>
<td></td>
<td>The following options are available for ECDSA:</td>
</tr>
<tr>
<td></td>
<td>• 256</td>
</tr>
<tr>
<td></td>
<td>• 384</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> RSA and ECDSA public keys might have different key length for the same security level.</td>
</tr>
<tr>
<td></td>
<td>Choose 2048 if you plan to get a public CA-signed certificate or deploy Cisco ISE as a FIPS-compliant policy management system.</td>
</tr>
<tr>
<td>Digest to Sign With</td>
<td>Choose one of the following hashing algorithm: SHA-1 or SHA-256.</td>
</tr>
<tr>
<td>Certificate Policies</td>
<td>Enter the certificate policy OID or list of OIDs that the certificate should conform to. Use comma or space to separate the OIDs.</td>
</tr>
<tr>
<td>Expiration TTL</td>
<td>Specify the number of days after which the certificate will expire.</td>
</tr>
<tr>
<td>Friendly Name</td>
<td>Enter a friendly name for the certificate. If you do not specify a name, Cisco ISE automatically creates a name in the format <code>&lt;common name&gt; # &lt;issuer&gt; # &lt;nnnnn&gt;</code> where <code>&lt;nnnnn&gt;</code> is a unique five-digit number.</td>
</tr>
<tr>
<td>Allow Wildcard Certificates</td>
<td>Check this check box if you want to generate a self-signed wildcard certificate (a certificate that contains an asterisk (*) in any Common Name in the Subject and/or the DNS name in the Subject Alternative Name. For example, DNS name assigned to the SAN can be *.amer.cisco.com.</td>
</tr>
</tbody>
</table>
Certificate-Signing Request Settings

Cisco ISE allows you to generate CSRs for all the nodes in your deployment from the Admin portal in a single request. Also, you can choose to generate the CSR for a single node or multiple both nodes in the deployment. If you choose to generate a CSR for a single node, ISE automatically substitutes the Fully Qualified Domain Name (FQDN) of the particular node in the CN= field of the certificate subject. If you choose to include an entry in the Subject Alternative Name (SAN) field of the certificate, you must enter the FQDN of the ISE node in addition to other SAN attributes. If you choose to generate CSRs for all the nodes in your deployment, check the Allow Wildcard Certificates check box and enter the wildcard FQDN notation in the SAN field (DNS name), for example, *.amer.example.com. If you plan to use the certificate for EAP Authentication, do not enter the wildcard value in the CN= field.

With the use of wildcard certificates, you no longer have to generate a unique certificate for each Cisco ISE node. Also, you no longer have to populate the SAN field with multiple FQDN values to prevent certificate warnings. Using an asterisk (*) in the SAN field allows you to share a single certificate across multiple both nodes in a deployment and helps prevent certificate name mismatch warnings. However, use of wildcard certificates is considered less secure than assigning a unique server certificate for each Cisco ISE node.

The following table describes the fields in the Certificate Signing Request (CSR) page, which you can use to generate a CSR that can be signed by a Certificate Authority (CA). The navigation path for this page is: Administration > System > Certificates > Certificate Management > Certificate Signing Request.
<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate(s) will be used for</td>
<td></td>
</tr>
</tbody>
</table>
### Certificate-Signing Request Settings

#### Field | Usage Guidelines
--- | ---

Choose the service for which you are going to use the certificate:

**Cisco ISE Identity Certificates**

- **Multi-Use**—Used for multiple services (Admin, EAP-TLS Authentication, pxGrid, and Portal). Multi-use certificates use both client and server key usages. The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties:
  - Key Usage: Digital Signature (Signing)
  - Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) and TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)

- **Admin**—Used for server authentication (to secure communication with the Admin portal and between ISE nodes in a deployment). The certificate template on the signing CA is often called a Web Server certificate template. This template has the following properties:
  - Key Usage: Digital Signature (Signing)
  - Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)

- **EAP Authentication**—Used for server authentication. The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties:
  - Key Usage: Digital Signature (Signing)
  - Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)

- **RADIUS DTLS**—Used for RADIUS DTLS server authentication. This template has the following properties:
  - Key Usage: Digital Signature (Signing)
  - Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)

- **Portal**—Used for server authentication (to secure communication with all ISE web portals). The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties:
  - Key Usage: Digital Signature (Signing)
  - Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)

- **pxGrid**—Used for both client and server authentication (to secure communication between the pxGrid client and server). The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties:
  - Key Usage: Digital Signature (Signing)

**Note**  
Digital signature key usage is required for EAP-TLS client certificates.
### Usage Guidelines

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) and TLS Web Client Authentication (1.3.6.1.5.5.7.3.2)</td>
</tr>
<tr>
<td></td>
<td>• SAML—Server certificate used to secure communication with the SAML Identity Provider (IdP). A certificate designated for SAML use cannot be used for any other service such as Admin, EAP authentication, etc.</td>
</tr>
<tr>
<td></td>
<td>• Key Usage: Digital Signature (Signing)</td>
</tr>
<tr>
<td></td>
<td>• Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)</td>
</tr>
<tr>
<td>Note</td>
<td>We recommend that you do not use a certificate that contains the value of 2.5.29.37.0 for the Any Purpose object identifier in the Extended Key Usage attribute. If you use a certificate that contains the value of 2.5.29.37.0 for the Any Purpose object identifier in the Extended Key Usage attribute, the certificate is considered invalid and the following error message is displayed:</td>
</tr>
<tr>
<td></td>
<td>source=local ; type=fatal ; message=&quot;unsupported certificate&quot;</td>
</tr>
</tbody>
</table>

### Cisco ISE Certificate Authority Certificates

|       | • ISE Root CA—(Applicable only for the internal CA service) Used for regenerating the entire internal CA certificate chain including the root CA on the Primary PAN and subordinate CAs on the PSNs. |
|       | • ISE Intermediate CA—(Applicable only for the internal CA service when ISE acts as an intermediate CA of an external PKI) Used to generate an intermediate CA certificate on the Primary PAN and subordinate CA certificates on the PSNs. The certificate template on the signing CA is often called a Subordinate Certificate Authority. This template has the following properties: |
|       | • Basic Constraints: Critical, Is a Certificate Authority |
|       | • Key Usage: Certificate Signing, Digital Signature |
|       | • Extended Key Usage: OCSP Signing (1.3.6.1.5.5.7.3.9) |
|       | • Renew ISE OCSP Responder Certificates—(Applicable only for the internal CA service) Used to renew the ISE OCSP responder certificate for the entire deployment (and is not a certificate signing request). For security reasons, we recommend that you renew the ISE OCSP responder certificates every six months. |

### Allow Wildcard Certificates

<p>| Allow Wildcard Certificates | Check this check box to use a wildcard character (<em>) in the CN and/or the DNS name in the SAN field of the certificate. If you check this check box, all the nodes in the deployment are selected automatically. You must use the asterisk (</em>) wildcard character in the left-most label position. If you use wildcard certificates, we recommend that you partition your domain space for greater security. For example, instead of *.example.com, you can partition it as *.amer.example.com. If you do not partition your domain, it can lead to security issues. |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate CSRs for these Nodes</td>
<td>Check the check boxes next to the nodes for which you want to generate the certificate. To generate a CSR for select nodes in the deployment, you must uncheck the Allow Wildcard Certificates option.</td>
</tr>
<tr>
<td>Common Name (CN)</td>
<td>By default, the common name is the FQDN of the ISE node for which you are generating the CSR. SFQDNS denotes the FQDN of the ISE node. When you generate CSRs for multiple nodes in the deployment, the Common Name field in the CSRs is replaced with the FQDN of the respective ISE nodes.</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>Organizational Unit name. For example, Engineering.</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Organization name. For example, Cisco.</td>
</tr>
<tr>
<td>City (L)</td>
<td>(Do not abbreviate) City name. For example, San Jose.</td>
</tr>
<tr>
<td>State (ST)</td>
<td>(Do not abbreviate) State name. For example, California.</td>
</tr>
<tr>
<td>Country (C)</td>
<td>Country name. You must enter the two-letter ISO country code. For example, US.</td>
</tr>
<tr>
<td>Subject Alternative Name (SAN)</td>
<td>An IP address, DNS name, Uniform Resource Identifier (URI), or Directory Name that is associated with the certificate.</td>
</tr>
<tr>
<td>Key Type</td>
<td>Specify the algorithm to be used for creating the public key: RSA or ECDSA.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

**Field** | **Usage Guidelines**
---|---
Key Length | Specify the bit size for the public key. The following options are available for RSA:
• 512
• 1024
• 2048
• 4096
The following options are available for ECDSA:
• 256
• 384

**Note** RSA and ECDSA public keys might have different key length for the same security level.

Choose 2048 or greater if you plan to get a public CA-signed certificate or deploy Cisco ISE as a FIPS-compliant policy management system.

**Digest to Sign With** | Choose one of the following hashing algorithm: SHA-1 or SHA-256.

**Certificate Policies** | Enter the certificate policy OID or list of OIDs that the certificate should conform to. Use comma or space to separate the OIDs.

### Related Topics
- Certificate Signing Requests, on page 156
- Create a Certificate Signing Request and Submit the CSR to a Certificate Authority, on page 156
- Bind the CA-Signed Certificate to the CSR, on page 157

### Issued and Revoked Certificates

The following table describes the fields on the Overview of Issued and Revoked Certificates page. The PSN nodes in your deployment issue certificates to endpoints. This page provides you information about the endpoint certificates issued by each of the PSN nodes in your deployment. The navigation path for this page is: Administration > System > Certificates > Overview.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Name</td>
<td>Name of the Policy Service node (PSN) that issued the certificate.</td>
</tr>
<tr>
<td>Certificates Issued</td>
<td>Number of endpoint certificates issued by the PSN node.</td>
</tr>
<tr>
<td>Certificates Revoked</td>
<td>Number of revoked endpoint certificates (certificates that were issued by the PSN node).</td>
</tr>
<tr>
<td>Certificates Requests</td>
<td>Number of certificate-based authentication requests processed by the PSN node.</td>
</tr>
<tr>
<td>Certificates Failed</td>
<td>Number of failed authentication requests processed by the PSN node.</td>
</tr>
</tbody>
</table>
Check the Status of the Certificates (OCSP or CRL).

Cisco ISE checks the Certificate Revocation Lists (CRL) periodically. Using this page, you can configure Cisco ISE to check ongoing sessions against CRLs that are downloaded automatically. You can specify the time of the day when the OCSP or CRL checks should begin each day and the time interval in hours that Cisco ISE waits before checking the OCSP server or CRLs again.

The following table describes the fields in the Certificate Periodic Check Settings page, which you can use to specify the time interval for checking the status of certificates (OCSP or CRL). The navigation path for this page is: Administration > System > Certificates > Certificate Management > Certificate Periodic Check Settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Check Settings</td>
<td>Check this checkbox if you want Cisco ISE to check ongoing sessions against CRLs that are automatically downloaded.</td>
</tr>
<tr>
<td>First check at</td>
<td>Specify the time of the day when the CRL or OCSP check should begin each day. Enter a value between 00:00 and 23:59 hours.</td>
</tr>
<tr>
<td>Check every</td>
<td>Specify the time interval in hours that Cisco ISE waits before checking the CRL or OCSP server again.</td>
</tr>
</tbody>
</table>

System Certificate Import Settings

The following table describes the fields in the Import System Certificate page that you can use to import a server certificate. The navigation path for this page is: Administration > System > Certificates > System Certificates > Import.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Node</td>
<td>(Required) Choose the Cisco ISE node on which you want to import the system certificate.</td>
</tr>
<tr>
<td>Certificate File</td>
<td>(Required) Click Browse to select the certificate file from your local system.</td>
</tr>
<tr>
<td>Private Key File</td>
<td>(Required) Click Browse to select the private key file.</td>
</tr>
</tbody>
</table>
### Fields

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password</strong></td>
</tr>
<tr>
<td><strong>Friendly Name</strong></td>
</tr>
<tr>
<td><strong>Allow Wildcard Certificates</strong></td>
</tr>
<tr>
<td><strong>Validate Certificate Extensions</strong></td>
</tr>
<tr>
<td><strong>Usage</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

### Related Topics

- System Certificates, on page 145
- View System Certificates, on page 146
- Import a System Certificate, on page 147

### Trusted Certificate Store Page

The following table describes the fields on the Trusted Certificates Store page, which you can use to view the certificates that are added to the Administration node. The navigation path for this page is: Administration > System > Certificates > Trusted Certificates.
### Table 74: Certificate Store Page

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friendly Name</td>
<td>Displays the name of the certificate.</td>
</tr>
<tr>
<td>Status</td>
<td>Enabled or Disabled. If Disabled, ISE will not use the certificate for establishing trust.</td>
</tr>
<tr>
<td>Trusted for</td>
<td>Displays the service for which the certificate is used.</td>
</tr>
<tr>
<td>Issued To</td>
<td>Common Name (CN) of the certificate subject.</td>
</tr>
<tr>
<td>Issued By</td>
<td>Common Name (CN) of the certificate issuer.</td>
</tr>
<tr>
<td>Valid From</td>
<td>The “Not Before” certificate attribute.</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>The “Not After” certificate attribute.</td>
</tr>
</tbody>
</table>

Expiration Status

Provides information about the status of the certificate expiration. There are five icons and categories of informational message that appear in this column:

- Green—Expiring in more than 90 days
- Blue—Expiring in 90 days or less
- Yellow—Expiring in 60 days or less
- Orange—Expiring in 30 days or less
- Red—Expired

### Related Topics
- Trusted Certificates Store, on page 150
- View Trusted Store Certificates, on page 153
- Change the Status of a Certificate in Trusted Certificates Store, on page 153
- Add a Certificate to Trusted Certificates Store, on page 153

### Edit Certificate Settings

The following table describes the fields on the Certificate Store Edit Certificate page, which you can use to edit the Certificate Authority (CA) certificate attributes. The navigation path for this page is: Administration > System > Certificates > Trusted Certificates > Certificate > Edit.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Issuer</td>
<td></td>
</tr>
<tr>
<td>Friendly Name</td>
<td>Enter a friendly name for the certificate.</td>
</tr>
<tr>
<td>Status</td>
<td>Choose Enabled or Disabled. If Disabled, ISE will not use the certificate for establishing trust.</td>
</tr>
</tbody>
</table>
### Fields

<table>
<thead>
<tr>
<th>Description</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>Enter an optional description.</td>
</tr>
<tr>
<td><strong>Usage</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Trust for authentication within ISE</strong></td>
<td>Check the check box if you want this certificate to verify server certificates (from other ISE nodes or LDAP servers).</td>
</tr>
</tbody>
</table>
| **Trust for client authentication and Syslog** | (Applicable only if you check the Trust for authentication within ISE check box) Check the check box if you want this certificate to be used to:  
  - Authenticate endpoints that connect to ISE using the EAP protocol  
  - Trust a Syslog server |
<p>| <strong>Trust for authentication of Cisco Services</strong> | Check this check box if you want this certificate to be used to trust external Cisco services such as the feed service. |
| <strong>Certificate Status Validation</strong> | ISE supports two ways of checking the revocation status of a client or server certificate that is issued by a particular CA. The first is to validate the certificate using the Online Certificate Status Protocol (OCSP), which makes a request to an OCSP service maintained by the CA. The second is to validate the certificate against a Certificate Revocation List (CRL) which is downloaded from the CA into ISE. Both of these methods can be enabled, in which case OCSP is used first, and only if a status determination cannot be made then the CRL is used. |
| <strong>Validate Against OCSP Service</strong> | Check the check box to validate the certificate against OCSP services. You must first create an OCSP Service to be able to check this box. |
| <strong>Reject the request if OCSP returns UNKNOWN status</strong> | Check the check box to reject the request if certificate status is not determined by OCSP. If you check this check box, an unknown status value returned by the OCSP service will cause ISE to reject the client or server certificate currently being evaluated. |
| <strong>Reject the request if OCSP Responder is unreachable</strong> | Check the check box for ISE to reject the request if the OCSP Responder is not reachable. |
| <strong>Download CRL</strong> | Check the check box for the Cisco ISE to download a CRL. |</p>
<table>
<thead>
<tr>
<th><strong>Fields</strong></th>
<th><strong>Usage Guidelines</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>CRL Distribution URL</td>
<td>Enter the URL to download the CRL from a CA. This field will be automatically populated if it is specified in the certificate authority certificate. The URL must begin with “http”, “https”, or “ldap.”</td>
</tr>
<tr>
<td>Retrieve CRL</td>
<td>The CRL can be downloaded automatically or periodically. Configure the time interval between downloads.</td>
</tr>
<tr>
<td>If download failed, wait</td>
<td>Configure the time interval to wait before Cisco ISE tries to download the CRL again.</td>
</tr>
<tr>
<td>Bypass CRL Verification if CRL is not Received</td>
<td>Check this check box, for the client requests to be accepted before the CRL is received. If you uncheck this check box, all client requests that use certificates signed by the selected CA will be rejected until Cisco ISE receives the CRL file.</td>
</tr>
<tr>
<td>Ignore that CRL is not yet valid or expired</td>
<td>Check this check box if you want Cisco ISE to ignore the start date and expiration date and continue to use the not yet active or expired CRL and permit or reject the EAP-TLS authentications based on the contents of the CRL. Uncheck this check box if you want Cisco ISE to check the CRL file for the start date in the Effective Date field and the expiration date in the Next Update field. If the CRL is not yet active or has expired, all authentications that use certificates signed by this CA are rejected.</td>
</tr>
</tbody>
</table>

**Related Topics**

- trusted certificates store, on page 150
- edit a trusted certificate, on page 154

**trusted certificate import settings**

The following table describes the fields on the Trusted Certificate Import page, which you can use to add Certificate Authority (CA) certificates to Cisco ISE. The navigation path for this page is: Administration > System > Certificates > Trusted Certificates > Import.

**Table 76: Trusted Certificate Import Settings**

<table>
<thead>
<tr>
<th><strong>Fields</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate File</td>
<td>Click <strong>Browse</strong> to choose the certificate file from the computer that is running the browser.</td>
</tr>
</tbody>
</table>
### Fields

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Friendly Name</td>
<td>Enter a friendly name for the certificate. If you do not specify a name, Cisco ISE automatically creates a name in the format &lt;common name&gt;#$&lt;issuer&gt;$#&lt;nmmm&gt;, where &lt;nmmm&gt; is a unique five-digit number.</td>
</tr>
<tr>
<td>Trust for authentication within ISE</td>
<td>Check the check box if you want this certificate to be used to verify server certificates (from other ISE nodes or LDAP servers).</td>
</tr>
</tbody>
</table>
| Trust for client authentication and Syslog | (Applicable only if you check the Trust for authentication within ISE check box) Check the check box if you want this certificate to be used to:  
  - Authenticate endpoints that connect to ISE using the EAP protocol  
  - Trust a Syslog server                                                                                                                                 |
| Trust for authentication of Cisco Services | Check this check box if you want this certificate to be used to trust external Cisco services such as the feed service.                                                                               |
| Validate Certificate Extensions      | (Only if you check both the Trust for client authentication and Enable Validation of Certificate Extensions options) Ensure that the “keyUsage” extension is present and the “keyCertSign” bit is set, and that the basic constraints extension is present with the CA flag set to true. |
| Description                          | Enter an optional description.                                                                                                                                                                              |

**Related Topics**

- [Trusted Certificates Store](#), on page 150
- [Certificate Chain Import](#), on page 155
- [Import the Root Certificates to the Trusted Certificate Store](#), on page 155

### OCSP Client Profile Settings

The following table describes the fields on the OCSP Client Profile page, which you can use to configure OCSP client profiles. The navigation path for this page is **Administration > Certificates > Certificate Management > OCSP Client Profile**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the OCSP Client Profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter an optional description.</td>
</tr>
</tbody>
</table>

**Configure OCSP Responder**
<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Secondary Server</td>
<td>Check this checkbox to enable a secondary OCSP server for high availability.</td>
</tr>
<tr>
<td>Always Access Primary Server First</td>
<td>Use this option to check the primary server before trying to move to the secondary server. Even if the primary was checked earlier and found to be unresponsive, Cisco ISE will try to send a request to the primary server before moving to the secondary server.</td>
</tr>
<tr>
<td>Fallback to Primary Server After Interval $n$ Minutes</td>
<td>Use this option when you want Cisco ISE to move to the secondary server and then fall back to the primary server again. In this case, all other requests are skipped, and the secondary server is used for the amount of time that is configured in the text box. The allowed time range is 1 to 999 minutes.</td>
</tr>
<tr>
<td><strong>Primary and Secondary Servers</strong></td>
<td></td>
</tr>
<tr>
<td>URL</td>
<td>Enter the URL of the primary and/or secondary OCSP server.</td>
</tr>
<tr>
<td>Enable Nonce Extension Support</td>
<td>You can configure a nonce to be sent as part of the OCSP request. The Nonce includes a pseudo-random number in the OCSP request. It is verified that the number that is received in the response is the same as the number that is included in the request. This option ensures that old communications cannot be reused in replay attacks.</td>
</tr>
<tr>
<td>Validate Response Signature</td>
<td>The OCSP responder signs the response with one of the following certificates:</td>
</tr>
<tr>
<td></td>
<td>• The CA certificate</td>
</tr>
<tr>
<td></td>
<td>• A certificate different from the CA certificate</td>
</tr>
<tr>
<td></td>
<td>In order for Cisco ISE to validate the response signature, the OCSP responder needs to send the response along with the certificate, otherwise the response verification fails, and the status of the certificate cannot be relied on. According to the RFC, OCSP can sign the response using different certificates. This is true as long as OCSP sends the certificate that signed the response for Cisco ISE to validate it. If OCSP signs the response with a different certificate that is not configured in Cisco ISE, the response verification will fail.</td>
</tr>
<tr>
<td>Use OCSP URLs specified in Authority Information Access (AIA)</td>
<td>Click the radio button to use the OCSP URLs specified in the Authority Information Access extension.</td>
</tr>
<tr>
<td><strong>Response Cache</strong></td>
<td></td>
</tr>
</tbody>
</table>
### Internal CA Settings

The following table describes the fields in the internal CA settings page. You can view the internal CA settings and disable the internal CA service from this page. The navigation path for this page is: Administration > System > Certificates > Internal CA Settings.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
</table>
| Cache Entry Time To Live n Minutes | Enter the time in minutes after which the cache entry expires. Each response from the OCSP server holds a `nextUpdate` value. This value shows when the status of the certificate will be updated next on the server. When the OCSP response is cached, the two values (one from the configuration and another from response) are compared, and the response is cached for the period of time that is the lowest value of these two. If the `nextUpdate` value is 0, the response is not cached at all. Cisco ISE will cache OCSP responses for the configured time. The cache is not replicated or persistent, so when Cisco ISE restarts, the cache is cleared. The OCSP cache is used in order to maintain the OCSP responses and for the following reasons:  
  - To reduce network traffic and load from the OCSP servers on an already-known certificate  
  - To increase the performance of Cisco ISE by caching already-known certificate statuses  
  
By default, the cache is set to 2 minutes for the internal CA OCSP client profile. If an endpoint authenticates a second time within 2 minutes of the first authentication, the OCSP cache is used and the OCSP responder is not queried. If the endpoint certificate has been revoked within the cache period, the previous OCSP status of Good will be used and the authentication succeeds. Setting the cache to 0 minutes prevents any responses from being cached. This option improves security, but decreases authentication performance. |
| Clear Cache | Click **Clear Cache** to clear entries of all the certificate authorities that are connected to the OCSP service. In a deployment, **Clear Cache** interacts with all the nodes and performs the operation. This mechanism updates every node in the deployment. |

### Related Topics

- [OCSP Services](#), on page 190
- [Cisco ISE CA Service Online Certificate Status Protocol Responder](#), on page 191
- [OCSP Certificate Status Values](#), on page 191
- [OCSP High Availability](#), on page 191
- [OCSP Failures](#), on page 192
- [OCSP Statistics Counters](#), on page 193
- [Add OCSP Client Profiles](#), on page 192
Certificate Template Settings

The following table describes the fields in the CA Certificate Template page, which you can use to define a SCEP RA profile that will be used by the client provisioning policy. The navigation path for this page is: Administration > System > Certificates > Certificate Templates > Add.

We do not support UTF-8 characters in the certificate template fields (Organizational Unit, Organization, City, State, and Country). Certificate provisioning fails if UTF-8 characters are used in the certificate template.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable Certificate Authority</td>
<td>Click this button to disable the internal CA service.</td>
</tr>
<tr>
<td>Host Name</td>
<td>Host name of the Cisco ISE node that is running the CA service.</td>
</tr>
<tr>
<td>Personas</td>
<td>Cisco ISE node personas that are enabled on the node running the CA service. For example, Administration, Policy Service, etc.</td>
</tr>
<tr>
<td>Role(s)</td>
<td>The role(s) assumed by the Cisco ISE node running the CA service. For example, Standalone or Primary or Secondary.</td>
</tr>
<tr>
<td>CA, EST &amp; OCSP Responder Status</td>
<td>Enabled or disabled</td>
</tr>
<tr>
<td>OCSP Responder URL</td>
<td>URL for Cisco ISE node to access the OCSP server.</td>
</tr>
<tr>
<td>SCEP URL</td>
<td>URL for the Cisco ISE node to access the SCEP server.</td>
</tr>
</tbody>
</table>

Related Topics
- Cisco ISE CA Service, on page 164
- Configure Cisco ISE to Use Certificates for Authenticating Personal Devices, on page 175

Certificate Template Settings

The following table describes the fields in the CA Certificate Template page, which you can use to define a SCEP RA profile that will be used by the client provisioning policy. The navigation path for this page is: Administration > System > Certificates > Certificate Templates > Add.

We do not support UTF-8 characters in the certificate template fields (Organizational Unit, Organization, City, State, and Country). Certificate provisioning fails if UTF-8 characters are used in the certificate template.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>(Required) Enter a name for the certificate template. For example, Internal_CA_Template.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description.</td>
</tr>
<tr>
<td>Common Name (CN)</td>
<td>(Display only) Common name is autopopulated with the username.</td>
</tr>
<tr>
<td>Organizational Unit (OU)</td>
<td>Organizational Unit name. For example, Engineering.</td>
</tr>
<tr>
<td>Organization (O)</td>
<td>Organization name. For example, Cisco.</td>
</tr>
<tr>
<td>City (L)</td>
<td>(Do not abbreviate) City name. For example, San Jose.</td>
</tr>
<tr>
<td>State (ST)</td>
<td>(Do not abbreviate) State name. For example, California.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country (C)</td>
<td>Country name. You must enter the two-letter ISO country code. For example, US.</td>
</tr>
<tr>
<td>Subject Alternative Name (SAN)</td>
<td>(Display only) MAC address of the endpoint.</td>
</tr>
<tr>
<td>Key Type</td>
<td>RSA or ECC</td>
</tr>
<tr>
<td>Key Size</td>
<td>(Applicable only if you choose RSA) Specify a key size of 1024 or higher.</td>
</tr>
<tr>
<td>Curve Type</td>
<td>(Applicable only if you choose ECC) Specify a curve type (the default is P-384).</td>
</tr>
<tr>
<td>SCEP RA Profile</td>
<td>Choose the ISE Internal CA or an external SCEP RA profile that you have created.</td>
</tr>
<tr>
<td>Valid Period</td>
<td>Enter the number of days after which the certificate expires.</td>
</tr>
</tbody>
</table>

**Extended Key Usage**
- **Client Authentication**: Check this check box if you want to use this certificate for client authentication.
- **Server Authentication**: Check this check box if you want to use this certificate for server authentication.

### Related Topics
- Certificate Templates, on page 169
- Certificate Template Name Extension, on page 169
- Configure Cisco ISE to Use Certificates for Authenticating Personal Devices, on page 175
- Deploy Cisco ISE CA Certificates for pxGrid Controller, on page 170
- Use Certificate Template Name in Authorization Policy Conditions, on page 170

## Logging Settings

These pages allow you to configure the severity of debug logs, create an external log target, and enable Cisco ISE to send log messages to these external log targets.

### Remote Logging Target Settings

The following table describes the fields on the Remote Logging Targets page, which you can use to create external locations (syslog servers) to store logging messages. The navigation path for this page is: Administration > System > Logging > Remote Logging Targets.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the new target.</td>
</tr>
<tr>
<td>Target Type</td>
<td>Select the target type. By default it is set to UDP Syslog.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a brief description of the new target.</td>
</tr>
</tbody>
</table>
### Remote Logging Target Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address or hostname of the destination machine where you want to store the logs.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number of the destination machine.</td>
</tr>
<tr>
<td>Facility Code</td>
<td>Choose the syslog facility code to be used for logging. Valid options are Local0 through Local7.</td>
</tr>
<tr>
<td>Maximum Length</td>
<td>Enter the maximum length of the remote log target messages. Valid options are from 200 to 1024 bytes.</td>
</tr>
<tr>
<td>Buffer Message When Server Down</td>
<td>Check this check-box if you want Cisco ISE to buffer the syslog messages when TCP syslog targets and secure syslog targets are unavailable. ISE retries sending the messages to the target when the connection resumes. After the connection resumes, messages are sent by the order from oldest to newest and buffered messages are always sent before new messages. If the buffer is full, old messages are discarded.</td>
</tr>
<tr>
<td>Buffer Size (MB)</td>
<td>Set the buffer size for each target. By default, it is set to 100 MB. Changing the buffer size clears the buffer and all existing buffered messages for the specific target are lost.</td>
</tr>
<tr>
<td>Reconnect Timeout (Sec)</td>
<td>Give in seconds how long will the TCP and secure syslogs be kept before being discarded, when the server is down.</td>
</tr>
<tr>
<td>Select CA Certificate</td>
<td>Select a client certificate.</td>
</tr>
<tr>
<td>Ignore Server Certificate Validation</td>
<td>Check this check-box if you want ISE to ignore server certificate authentication and accept any syslog server. By default, this option is set to off unless the system is in FIPS mode when this is disabled.</td>
</tr>
</tbody>
</table>

### Related Topics
- Cisco ISE Logging Mechanism, on page 267
- Cisco ISE System Logs, on page 268
- Remote Syslog Message Format, on page 270
- Cisco ISE Message Catalogs, on page 274
- Collection Filters, on page 276
- Event Suppression Bypass Filter, on page 276
- Configure Remote Syslog Collection Locations, on page 272
- Configure Collection Filters, on page 276
The following table describes the fields on the Logging Categories page, which you can use to configure the log severity level and choose logging targets for the logs of selected categories to be stored. The navigation path for this page is: Administration > System > Logging > Logging Categories.

**Table 78: Logging Category Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the name of the logging category.</td>
</tr>
</tbody>
</table>
| Log Severity Level | Allows you to choose the severity level for the diagnostic logging categories from the following options:  
  - **FATAL**—Emergency. This option means that Cisco ISE cannot be used and you must take action immediately  
  - **ERROR**—This option indicates a critical or error condition.  
  - **WARN**—This option indicates a normal but significant condition. This is the default condition.  
  - **INFO**—This option indicates an informational message.  
  - **DEBUG**—This option indicates a diagnostic bug message. |
| Local Logging   | Check this check box to enable logging event for the category on the local node.  |
| Target          | Allows you to change the targets for a category by transferring the targets between the Available and the Selected boxes using the left and right icons. The Available box contains the existing logging targets, both local (predefined) and external (user-defined). The Selected box, which is initially empty, contains the selected targets for the specific category. |

**Related Topics**
- [Remote Syslog Message Format](#), on page 270
- [Cisco ISE Message Codes](#), on page 273
- [Configure Remote Syslog Collection Locations](#), on page 272
- [Set Severity Levels for Message Codes](#), on page 273
Maintenance Settings

These pages help you to manage data using the backup, restore, and data purge features.

Repository Settings

The following table describes the fields on the Repository List page, which you can use to create repositories to store your backup files. The navigation path for this page is: Administration > System > Maintenance > Repository.

Table 79: Repository Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repository</td>
<td>Enter the name of the repository. Alphanumeric characters are allowed and the maximum length is 80 characters.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Choose one of the available protocols that you want to use.</td>
</tr>
<tr>
<td>Server Name</td>
<td>(Required for TFTP, HTTP, HTTPS, FTP, SFTP, and NFS) Enter the hostname or IPv4 address of the server where you want to create the repository.</td>
</tr>
<tr>
<td>Path</td>
<td>Enter the path to your repository. The path must be valid and must exist at the time you create the repository.</td>
</tr>
<tr>
<td></td>
<td>This value can start with two forward slashes (//) or a single forward slash (/) denoting the root directory of the server. However, for the FTP protocol, a single forward slash (/) denotes the FTP user's home directory and not the root directory.</td>
</tr>
<tr>
<td>Enable PKI authentication</td>
<td>(Optional; applicable only for SFTP repository) Check this check box if you want to enable RSA Public Key Authentication in SFTP repository.</td>
</tr>
<tr>
<td>User Name</td>
<td>(Required for FTP, SFTP, and NFS) Enter the username that has write permission to the specified server. Only alphanumeric characters are allowed.</td>
</tr>
<tr>
<td>Password</td>
<td>(Required for FTP, SFTP, and NFS) Enter the password that will be used to access the specified server. Passwords can consist of the following characters: 0 through 9, a through z, A through Z, -, ., @, #, $, %, ^, &amp;, *, (, ), +, and =.</td>
</tr>
</tbody>
</table>
### Table 80: Repository Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repository</td>
<td>Enter the name of the repository. Alphanumeric characters are allowed and the maximum length is 80 characters.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Choose one of the available protocols that you want to use.</td>
</tr>
<tr>
<td>Host</td>
<td>(Required for TFTP, HTTP, HTTPS, FTP, SFTP, and NFS) Enter the hostname or IPv4 address of the server where you want to create the repository.</td>
</tr>
<tr>
<td>Path</td>
<td>Enter the path to your repository. The path must be valid and must exist at the time you create the repository. This value can start with two forward slashes (/) or a single forward slash (/) denoting the root directory of the server. However, for the FTP protocol, a single forward slash (/) denotes the FTP user's home directory and not the root directory.</td>
</tr>
</tbody>
</table>

**Related Topics**
- [Backup and Restore Repositories](#), on page 280
- [Create Repositories](#), on page 280

### On-Demand Backup Settings

The following table describes the fields on the On-Demand Backup page, which you can use to obtain a backup at any point of time. The navigation path for this page is: Administration > System > Backup & Restore.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Name</td>
<td>Enter the name of your backup file.</td>
</tr>
<tr>
<td>Repository Name</td>
<td>Repository where your backup file should be saved. You cannot enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before you run a backup.</td>
</tr>
<tr>
<td>Encryption Key</td>
<td>This key is used to encrypt and decrypt the backup file.</td>
</tr>
</tbody>
</table>

**Related Topics**
- [Backup Data Type](#), on page 279
- [On-Demand and Scheduled Backups](#), on page 282
Backup History, on page 286
Backup Failures, on page 286
Cisco ISE Restore Operation, on page 287
Export Authentication and Authorization Policy Configuration, on page 293
Synchronize Primary and Secondary Nodes in a Distributed Environment, on page 294
Perform an On-Demand Backup, on page 283

Scheduled Backup Settings

The following table describes the fields on the Scheduled Backup Page, which you can use to restore a full or incremental backup. The navigation path for this page is: Administration > System > Backup and Restore.

Table 82: Scheduled Backup Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for your backup file. You can enter a descriptive name of your choice. Cisco ISE appends the timestamp to the backup filename and stores it in the repository. You will have unique backup filenames even if you configure a series of backups. On the Scheduled Backup list page, the backup filename will be prepended with “backup_occur” to indicate that the file is a kron occurrence job.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the backup.</td>
</tr>
<tr>
<td>Repository Name</td>
<td>Select the repository where your backup file should be saved. You cannot enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before you run a backup.</td>
</tr>
<tr>
<td>Encryption Key</td>
<td>Enter a key to encrypt and decrypt the backup file.</td>
</tr>
<tr>
<td>Schedule Options</td>
<td>Choose the frequency of your scheduled backup and fill in the other options accordingly.</td>
</tr>
</tbody>
</table>

Related Topics

Backup Data Type, on page 279
On-Demand and Scheduled Backups, on page 282
Backup History, on page 286
Backup Failures, on page 286
Cisco ISE Restore Operation, on page 287
Export Authentication and Authorization Policy Configuration, on page 293
Synchronize Primary and Secondary Nodes in a Distributed Environment, on page 294
Backup Using the CLI, on page 286
Schedule a Backup, on page 284
Schedule Policy Export Settings

The following table describes the fields on the Schedule Policy Export page. The navigation path for this page is: Administration > System > Backup and Restore > Policy Export.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td></td>
</tr>
<tr>
<td>Encryption Key</td>
<td>Enter a key to encrypt and decrypt the export data. This field will be enabled only if you select the Export with Encryption Key option.</td>
</tr>
<tr>
<td>Destination</td>
<td></td>
</tr>
<tr>
<td>Download file to local computer</td>
<td>Allows you to download the policy export file to your local system.</td>
</tr>
<tr>
<td>Email file to</td>
<td>Enter multiple email addresses separated by a comma.</td>
</tr>
<tr>
<td>Repository</td>
<td>Select the repository where your export data should be saved. You cannot enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before scheduling the policy export.</td>
</tr>
<tr>
<td>Export Now</td>
<td>Click this option to export the data to the specified repository immediately.</td>
</tr>
<tr>
<td>Schedule</td>
<td></td>
</tr>
<tr>
<td>Schedule Options</td>
<td>Choose the frequency of the export schedule and enter the other details accordingly.</td>
</tr>
</tbody>
</table>

Admin Access Settings

These pages enable you to configure access settings for administrators.

Administrator Password Policy Settings

The following table describes the fields on the Administrator Password Policy page, which you can use to define a criteria that administrator passwords should meet. The navigation path for this page is: Administration > System > Admin Access > Authentication > Password Policy.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Length</td>
<td>Specifies the minimum length of the password (in characters). The default is six characters.</td>
</tr>
<tr>
<td><strong>Fields</strong></td>
<td><strong>Usage Guidelines</strong></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password must not contain</td>
<td>Admin name or its characters in reverse order—Check this check box to restrict the use of the administrator username or its characters in reverse order.</td>
</tr>
<tr>
<td></td>
<td>&quot;cisco&quot; or its characters in reverse order—Check this check box to restrict the use of the word &quot;cisco&quot; or its characters in reverse order.</td>
</tr>
<tr>
<td></td>
<td>This word or its characters in reverse order—Check this check box to restrict the use of any word that you define or its characters in reverse order.</td>
</tr>
<tr>
<td></td>
<td>Repeated characters four or more times consecutively—Check this check box to restrict the use of repeated characters four or more times consecutively.</td>
</tr>
<tr>
<td></td>
<td>Dictionary words, their characters in reverse order or their letters replaced with other characters—Check this check box to restrict the use of dictionary words, their characters in reverse order or their letters replaced with other characters.</td>
</tr>
<tr>
<td></td>
<td>Substitution of &quot;$&quot; for &quot;s&quot;, &quot;@&quot; for &quot;a&quot;, &quot;0&quot; for &quot;o&quot;, &quot;1&quot; for &quot;l&quot;, &quot;!&quot; for &quot;i&quot;, &quot;3&quot; for &quot;e&quot; is not permitted. For example, Pa$$w0rd</td>
</tr>
<tr>
<td></td>
<td>• Default Dictionary—Choose this option to use the default Linux dictionary in Cisco ISE. The default dictionary contains approximately 480,000 English words. By default, this option is selected.</td>
</tr>
<tr>
<td></td>
<td>• Custom Dictionary—Choose this option to use your customized dictionary. Click <strong>Choose File</strong> to select the custom dictionary file. The text file must be of newline-delimited words, .dic extension, and size less than 20 MB.</td>
</tr>
<tr>
<td>Required Characters</td>
<td>Specifies that the administrator password must contain at least one character of the type that you choose from the following choices:</td>
</tr>
<tr>
<td></td>
<td>• Lowercase alphabetic characters</td>
</tr>
<tr>
<td></td>
<td>• Uppercase alphabetic characters</td>
</tr>
<tr>
<td></td>
<td>• Numeric characters</td>
</tr>
<tr>
<td></td>
<td>• Non-alphanumeric characters</td>
</tr>
</tbody>
</table>
### Password History
Specifies the number of previous passwords from which the new password must be different to prevent the repeated use of the same password.
Also, specifies the number of characters that must be different from the previous password.
Enter the number of days before which you cannot reuse a password.

### Password Lifetime
Specifies the following options to force users to change passwords after a specified time period:
- Time (in days) before the administrator account is disabled if the password is not changed. (The allowable range is 0 to 2,147,483,647 days.)
- Reminder (in days) before the administrator account is disabled.

### Related Topics
- Cisco ISE Administrators, on page 99
- Create a New Cisco ISE Administrator, on page 100

### Session Timeout and Session Information Settings
The following table describes the fields on the Session page, which you can use to define session timeout and terminate an active administrative session. The navigation path for this page is: Administration > System > Admin Access > Settings > Session.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Timeout</td>
<td>Enter the time in minutes that you want Cisco ISE to wait before it logs out the administrator if there is no activity. The default value is 60 minutes. The valid range is from 6 to 100 minutes.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Info</td>
<td></td>
</tr>
<tr>
<td>Invalidate</td>
<td>Check the check box next to the session ID that you want to terminate and click <strong>Invalidate</strong>.</td>
</tr>
</tbody>
</table>

### Related Topics

- [Administrator Access Settings](#), on page 117
- [Configure Session Timeout for Administrators](#), on page 120
- [Terminate an Active Administrative Session](#), on page 120

### Settings

These pages enable you to configure general settings for the various services.

### Posture General Settings

The following table describes the fields on the Posture General Settings page, which you can use to configure general posture settings such as remediation time and posture status. The navigation path for this page is: *Administration > System > Settings > Posture > General Settings*.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediation Timer</td>
<td>Enter a time value in minutes. The default value is 4 minutes. The valid range is 1 to 300 minutes.</td>
</tr>
<tr>
<td>Network Transition Delay</td>
<td>Enter a time value in seconds. The default value is 3 seconds. The valid range is 2 to 30 seconds.</td>
</tr>
<tr>
<td>Default Posture Status</td>
<td>Choose Compliant or Noncompliant. The non-agent devices like Linux assumes this status while connecting to the network.</td>
</tr>
<tr>
<td>Automatically Close Login Success Screen After</td>
<td>Check the check box to close the login success screen automatically after the specified time. Enter a time value in seconds, in the field next to the check box. You can configure the timer to close the login screen automatically between 0 to 300 seconds. If the time is set to zero, then the NAC Agents and Web Agents do not display the login success screen.</td>
</tr>
<tr>
<td>Continuous Monitoring Interval</td>
<td>Specify the time interval after which AnyConnect should start sending monitoring data. For application condition For application and hardware conditions, the default value is 5 minutes.</td>
</tr>
</tbody>
</table>
### Posture Reassessment Configuration Settings

The following table describes the fields in the Posture Reassessment Configurations Page, which you can use to configure posture reassessment. The navigation path for this page is: Administration > System > Settings > Posture > Reassessments.

#### Table 87: Posture Reassessment Configuration Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Name</td>
<td>Enter the name of PRA configuration.</td>
</tr>
<tr>
<td>Configuration Description</td>
<td>Enter a description for PRA configuration.</td>
</tr>
<tr>
<td>Use Reassessment Enforcement?</td>
<td>Check the check box to apply the PRA configurations for the user identity groups.</td>
</tr>
</tbody>
</table>

---

**Usage Guidelines**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable Use Policy in Stealth Mode</td>
<td>Choose <strong>Block</strong> in stealth mode to move a client to noncompliant posture status, if your company's network-usage terms and conditions are not met.</td>
</tr>
<tr>
<td>Posture Lease</td>
<td>Select this option to initiate posture assessment every time the user connects to network</td>
</tr>
<tr>
<td>Perform posture assessment every time a user connects to the network</td>
<td>Select this option to initiate posture assessment every n days although the client is already postured Compliant.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Enforcement Type</td>
<td>Choose the action to be enforced:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Continue</strong> — The user continues to have the privileged access without any user intervention to remediate the client irrespective of the posture requirement.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Logoff</strong> — If the client is not compliant, the user is forced to logoff from the network. When the client logs in again, the compliance status is unknown.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remediate</strong> — If the client is not compliant, the agent waits for a specified time for the remediation to happen. Once the client has remediated, the agent sends the PRA report to the policy service node. If the remediation is ignored on the client, then the agent sends a logoff request to the policy service node to force the client to logoff from the network.</td>
</tr>
<tr>
<td></td>
<td>If the posture requirement is set to mandatory, then the RADIUS session will be cleared as a result of the PRA failure action and a new RADIUS session has to start for the client to be postured again.</td>
</tr>
<tr>
<td></td>
<td>If the posture requirement is set to optional, then the NAC Agent allows the user to click the continue option from the agent. The user can continue to stay in the current network without any restriction.</td>
</tr>
<tr>
<td>Interval</td>
<td>Enter a time interval in minutes to initiate PRA on the clients after the first successful login.</td>
</tr>
<tr>
<td></td>
<td>The default value is 240 minutes. Minimum value is 60 minutes and maximum is 1440 minutes.</td>
</tr>
<tr>
<td>Grace time</td>
<td>Enter a time interval in minutes to allow the client to complete remediation. The grace time cannot be zero, and should be greater than the PRA interval. It can range between the default minimum interval (5 minutes) and the minimum PRA interval.</td>
</tr>
<tr>
<td></td>
<td>The minimum value is 5 minutes and the maximum value is 60 minutes.</td>
</tr>
</tbody>
</table>
|                        | **Note** The grace time is enabled only when the enforcement type is set to remediate action after the client fails the posture reassessment.
### Usage Guidelines

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select User Identity Groups</td>
<td>Choose a unique group or a unique combination of groups for your PRA configuration.</td>
</tr>
<tr>
<td>PRA configurations</td>
<td>Displays existing PRA configurations and user identity groups associated to PRA configurations.</td>
</tr>
</tbody>
</table>

### Related Topics

- Posture Lease, on page 778
- Periodic Reassessments, on page 778
- Posture Assessment Options
- Posture Remediation Options, on page 790
- Custom Conditions for Posture, on page 791
- Custom Posture Remediation Actions, on page 792
- Configure Periodic Reassessments, on page 778

### Posture Acceptable Use Policy Configuration Settings

The following table describes the fields in the Posture Acceptable Use Policy Configurations Page, which you can use to configure an acceptable use policy for posture. The navigation path for this page is: Administration > System > Settings > Posture > Acceptable Use Policy.

#### Table 88: Posture AUP Configurations Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Name</td>
<td>Enter the name of the AUP configuration that you want to create.</td>
</tr>
<tr>
<td>Configuration Description</td>
<td>Enter the description of the AUP configuration that you want to create.</td>
</tr>
<tr>
<td>Show AUP to Agent users (for NAC Agent and Web Agent on Windows only)</td>
<td>If checked, the Show AUP to Agent users check box displays users (for NAC Agents, and Web Agents on Windows only) the link to network usage terms and conditions for your network and click it to view the AUP upon successful authentication and posture assessment.</td>
</tr>
<tr>
<td>Use URL for AUP message radio button</td>
<td>When selected, you must enter the URL to the AUP message in the AUP URL, which clients must access upon successful authentication and posture assessment.</td>
</tr>
<tr>
<td>Use file for AUP message radio button</td>
<td>When selected, you must browse to the location and upload a file in a zipped format in the AUP File, which contains the index.html at the top level. The .zip file can include other files and subdirectories in addition to the index.html file. These files can reference each other using HTML tags.</td>
</tr>
</tbody>
</table>
## Posture Acceptable Use Policy Configuration Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUP URL</td>
<td>Enter the URL to the AUP, which clients must access upon successful authentication and posture assessment.</td>
</tr>
<tr>
<td>AUP File</td>
<td>In the AUP File, browse to the file and upload it to the Cisco ISE server. It should be a zipped file and the zipped file should contain the index.html file at the top level.</td>
</tr>
<tr>
<td>Select User Identity Groups</td>
<td>In the Select User Identity Groups drop-down list, choose a unique user identity group, or a unique combination of user identity groups, for your AUP configuration.</td>
</tr>
<tr>
<td></td>
<td>Note the following while creating an AUP configuration:</td>
</tr>
<tr>
<td></td>
<td>* Posture AUP is not applicable for a guest flow</td>
</tr>
<tr>
<td></td>
<td>* Each configuration must have a unique user identity group, or a unique combination of user identity groups</td>
</tr>
<tr>
<td></td>
<td>* No two configurations have any user identity group in common</td>
</tr>
<tr>
<td></td>
<td>* If you want to create a AUP configuration with a user identity group “Any”, then delete all other AUP configurations first</td>
</tr>
<tr>
<td></td>
<td>* If you create a AUP configuration with a user identity group “Any”, then you cannot create other AUP configurations with a unique user identity group, or user identity groups. To create an AUP configuration with a user identity group other than Any, either delete an existing AUP configuration with a user identity group “Any” first, or update an existing AUP configuration with a user identity group “Any” with a unique user identity group, or user identity groups.</td>
</tr>
</tbody>
</table>

| Acceptable use policy configurations—Configurations list | Lists existing AUP configurations and end user identity groups associated with AUP configurations. |

### Related Topics
- [Posture Service](#)
- [Configure Acceptable Use Policies for Posture Assessment](#)
## EAP-FAST Settings

The following table describes the fields on the Protocol Settings page, which you can use to configure the EAP-FAST, EAP-TLS, and PEAP protocols. The navigation path for this page is: Administration > System > Settings > Protocols > EAP-FAST > EAP FAST Settings.

### Table 89: Configuring EAP-FAST Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority Identity Info Description</td>
<td>Enter a user-friendly string that describes the Cisco ISE node that sends credentials to a client. The client can discover this string in the Protected Access Credentials (PAC) information for type, length, and value (TLV). The default value is Identity Services Engine.</td>
</tr>
<tr>
<td>Master Key Generation Period</td>
<td>Specifies the master key generation period in seconds, minutes, hours, days, or weeks. The value must be a positive integer in the range 1 to 2147040000 seconds. The default is 604800 seconds, which is equivalent to one week.</td>
</tr>
<tr>
<td>Revoke all master keys and PACs</td>
<td>Click Revoke to revoke all master keys and PACs.</td>
</tr>
<tr>
<td>Enable PAC-less Session Resume</td>
<td>Check this check box if you want to use EAP-FAST without the PAC files.</td>
</tr>
<tr>
<td>PAC-less Session Timeout</td>
<td>Specifies the time in seconds after which the PAC-less session resume times out. The default is 7200 seconds.</td>
</tr>
</tbody>
</table>

### Related Topics
- Policy Set Protocol Settings, on page 579
- Guidelines for Using EAP-FAST as Protocol, on page 579
- Benefits of EAP-FAST, on page 1180
- Configure EAP-FAST Settings, on page 580

## Generate PAC for EAP-FAST Settings

The following table describes the fields on the Generate PAC page, which you can use to configure protected access credentials for EAP-FAST authentication. The navigation path for this page is: Administration > System > Settings > Protocols > EAP-FAST > Generate PAC.

### Table 90: Generating PAC for EAP-FAST Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel PAC</td>
<td>Click this radio button to generate a tunnel PAC.</td>
</tr>
<tr>
<td>Machine PAC</td>
<td>Click this radio button to generate a machine PAC.</td>
</tr>
<tr>
<td>Trustsec PAC</td>
<td>Click this radio button to generate a Trustsec PAC.</td>
</tr>
</tbody>
</table>
### EAP-TTLS Settings

The following table describes the fields on the EAP-TTLS Settings page. The navigation path for this page is: Administration > System > Settings > Protocols > EAP-TTLS.

<table>
<thead>
<tr>
<th><strong>Fields</strong></th>
<th><strong>Usage Guidelines</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
<td>(For the Tunnel and Machine PAC identity field) Specifies the username or machine name that is presented as the “inner username” by the EAP-FAST protocol. If the identity string does not match that username, authentication fails. This is the hostname as defined on the Adaptive Security Appliance (ASA). The identity string must match the ASA hostname otherwise, ASA cannot import the PAC file that is generated. If you are generating a Trustsec PAC, the Identity field specifies the Device ID of a Trustsec network device and is provided with an initiator ID by the EAP-FAST protocol. If the Identity string entered here does not match that Device ID, authentication fails.</td>
</tr>
<tr>
<td>PAC Time to Live</td>
<td>(For the Tunnel and Machine PAC) Enter a value in seconds that specifies the expiration time for the PAC. The default is 604800 seconds, which is equivalent to one week. This value must be a positive integer between 1 and 157680000 seconds. For the Trustsec PAC, enter a value in days, weeks, months, or years. By default, the value is one year. The minimum value is one day and the maximum is 10 years.</td>
</tr>
<tr>
<td>Encryption Key</td>
<td>Enter an encryption key. The length of the key must be between 8 and 256 characters. The key can contain uppercase or lowercase letters, or numbers, or a combination of alphanumeric characters.</td>
</tr>
<tr>
<td>Expiration Data</td>
<td>(For Trustsec PAC only) The expiration date is calculated based on the PAC Time to Live.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Policy Set Protocol Settings, on page 579
- Guidelines for Using EAP-FAST as Protocol, on page 579
- Generate the PAC for EAP-FAST, on page 580
Table 91: EAP-TTLS Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable EAP-TTLS Session Resume</td>
<td>If you check this check box, Cisco ISE will cache the TLS session that is created during phase one of EAP-TTLS authentication, provided the user successfully authenticates in phase two of EAP-TTLS. If a user needs to reconnect and the original EAP-TTLS session has not timed out, Cisco ISE uses the cached TLS session, resulting in faster EAP-TTLS performance and a reduced AAA server load. Note: When the EAP-TTLS session is resumed, the inner method is skipped.</td>
</tr>
<tr>
<td>EAP-TTLS Session Timeout</td>
<td>Specifies the time in seconds after which the EAP-TTLS session times out. The default value is 7200 seconds.</td>
</tr>
</tbody>
</table>

Related Topics
- Policy Set Protocol Settings, on page 579
- Using EAP-TTLS as Authentication Protocol, on page 580
- Configure EAP-TTLS Settings, on page 581

EAP-TLS Settings

The following table describes the fields on the EAP-TLS Settings page, which you can use to configure the EAP-TLS protocol settings. The navigation path for this page is: Administration > System > Settings > Protocols > EAP-TLS.

Table 92: EAP-TLS Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable EAP-TLS Session Resume</td>
<td>Check this check box to support an abbreviated reauthentication of a user who has passed full EAP-TTLS authentication. This feature provides reauthentication of the user with only a Secure Sockets Layer (SSL) handshake and without applying the certificates. EAP-TLS session resume works only if the EAP-TLS session has not timed out.</td>
</tr>
<tr>
<td>EAP-TLS Session Timeout</td>
<td>Specifies the time in seconds after which the EAP-TTLS session times out. The default value is 7200 seconds.</td>
</tr>
<tr>
<td>Stateless Session Resume</td>
<td></td>
</tr>
<tr>
<td>Master Key Generation Period</td>
<td>Enter the time after which the master key is regenerated. This value determines the duration that a master key remains active. You can enter the value in seconds, minutes, hours, days, or weeks.</td>
</tr>
</tbody>
</table>
PEAP Settings

The following table describes the fields on the PEAP Settings page, which you can use to configure the PEAP protocol settings. The navigation path for this page is: Administration > System > Settings > Protocols > PEAP.

**Table 93: PEAP Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revoke</td>
<td>Click Revoke to cancel all previously generated master keys and tickets. This option is disabled on the secondary node.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Policy Set Protocol Settings, on page 579
- Configure EAP-TLS Settings, on page 581

RADIUS Settings

The following table describes the fields on the RADIUS Settings page. The navigation path for this page is: Administration > System > Settings > Protocols > RADIUS.

If you enable the Suppress Repeated Failed Clients option, clients with repeated authentication failures will be suppressed from the audit logs, and the requests from these clients will be automatically rejected for the
specified time period. You can also specify the number of authentication failures after which the requests from these clients should be rejected. For example, if this value is configured as 5, when a client authentication fails five times, all the requests received from that client will be rejected for the configured time period.

Table 94: RADIUS Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppress Repeated Failed Clients</td>
<td>Check this check box to suppress the clients for which the authentications fail repeatedly for the same reason. These clients are suppressed from the audit logs and the requests from these clients are rejected for the specified time period if Reject RADIUS Requests from Clients with Repeated Failures option is enabled.</td>
</tr>
<tr>
<td>Detect Two Failures Within</td>
<td>Enter the time interval in minutes. If a client fails authentication twice for the same reason within this time period, it will be suppressed from the audit logs, and the requests from this client will be rejected if Reject RADIUS Requests from Clients with Repeated Failures option is enabled.</td>
</tr>
<tr>
<td>Report Failures Once Every</td>
<td>Enter the time interval in minutes for the failed authentications to be reported. For example, if this value is set as 15 minutes, clients that repeatedly fail authentication will be reported in the audit logs only once every 15 minutes, thereby preventing over-reporting.</td>
</tr>
<tr>
<td>Reject RADIUS Requests from Clients with Repeated Failures</td>
<td>Check this check box to automatically reject the RADIUS requests from the clients for which the authentications fail repeatedly. You can enable this option to avoid unnecessary processing by Cisco ISE and to protect against potential denial of service attacks.</td>
</tr>
<tr>
<td>Failures Prior to Automatic Rejection</td>
<td>Enter the number of authentication failures after which requests from clients with repeated failures are automatically rejected. All the requests received from these clients are automatically rejected for the configured time period (specified in Continue Rejecting Requests for field). After the interval expires, the authentication requests from these clients are processed.</td>
</tr>
<tr>
<td>Continue Rejecting Requests for</td>
<td>Enter the time interval (in minutes) for which the requests from clients with repeated failures are to be rejected.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ignore Repeated Accounting Updates Within</td>
<td>Repeated accounting updates that occur within this period will be ignored.</td>
</tr>
<tr>
<td>Suppress Successful Reports</td>
<td></td>
</tr>
<tr>
<td>Suppress Repeated Successful Authentications</td>
<td>Check this check box to prevent repeated reporting of successful authentication requests in last 24 hours that have no change in identity context, network device, and authorization.</td>
</tr>
<tr>
<td>Authentications Details</td>
<td></td>
</tr>
<tr>
<td>Highlight Steps Longer Than</td>
<td>Enter the time interval in milliseconds. If execution of a single step exceeds the specified threshold, it will be marked with a clock icon in the authentication details page.</td>
</tr>
<tr>
<td>RADIUS UDP Ports</td>
<td></td>
</tr>
<tr>
<td>Authentication Ports</td>
<td>Specify the ports to be used for RADIUS UDP authentication flows. You can specify a maximum of 4 port numbers (separated by a comma). By default, port 1812 and port 1645 are used. The valid range is from 1024 to 65535.</td>
</tr>
<tr>
<td>Accounting Ports</td>
<td>Specify the ports to be used for RADIUS UDP accounting flows. You can specify a maximum of 4 port numbers (separated by a comma). By default, port 1813 and port 1646 are used. The valid range is from 1024 to 65535.</td>
</tr>
<tr>
<td>Note</td>
<td>Ensure that these ports are not used by other services.</td>
</tr>
<tr>
<td>RADIUS DTLS</td>
<td></td>
</tr>
<tr>
<td>Authentication and Accounting Port</td>
<td>Specify the port to be used for RADIUS DTLS authentication and accounting flows. By default, port 2083 is used. The valid range is from 1024 to 65535.</td>
</tr>
<tr>
<td>Note</td>
<td>Ensure that this port is not used by other services.</td>
</tr>
<tr>
<td>Idle Timeout</td>
<td>Enter the time (in seconds) that you want Cisco ISE to wait before it closes the TLS session if no packets are received from the network device. Default value is 120 seconds. The valid range is from 60 to 600 seconds.</td>
</tr>
</tbody>
</table>
Enabling RADIUS/DTLS Client Identity Verification

Check this check box if you want Cisco ISE to verify the identity of the RADIUS/DTLS clients during the DTLS handshake. Cisco ISE fails the handshake if the client identity is not valid. Identity check is skipped for the default network device, if configured.

Identity check is performed in the following sequence:

1. If the client certificate contains the subject alternative name (SAN) attribute:
   • If SAN contains the DNS name, the DNS name specified in the certificate is compared with the DNS name that is configured for the network device in Cisco ISE.
   • If SAN contains the IP address (and does not contain the DNS name), the IP address specified in the certificate is compared with all the device IP addresses configured in Cisco ISE.

2. If the certificate does not contain SAN, subject CN is compared with the DNS name that is configured for the network device in Cisco ISE. Cisco ISE fails the handshake in the case of mismatch.

Related Topics

- Policy Set Protocol Settings, on page 579
- RADIUS Protocol Support in Cisco ISE, on page 1174
- Configure RADIUS Settings, on page 582

General TrustSec Settings

You must define the global TrustSec settings for Cisco ISE to function as a TrustSec server and provide TrustSec services. The following table describes the fields in the TrustSec Settings window (Work Centers > TrustSec > Settings > General TrustSec Settings).
<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tunnel PAC Time to Live</strong></td>
<td>Specify the expiry time for the PAC. The tunnel PAC generates a tunnel for the EAP-FAST protocol. You can specify the time in seconds, minutes, hours, days, or weeks. The default value is 90 days. The following are the valid ranges:</td>
</tr>
<tr>
<td></td>
<td>• 1 - 157680000 seconds</td>
</tr>
<tr>
<td></td>
<td>• 1 - 2628000 minutes</td>
</tr>
<tr>
<td></td>
<td>• 1 - 43800 hours</td>
</tr>
<tr>
<td></td>
<td>• 1 - 1825 days</td>
</tr>
<tr>
<td></td>
<td>• 1 - 260 weeks</td>
</tr>
<tr>
<td><strong>Proactive PAC Update Will Occur After</strong></td>
<td>Cisco ISE proactively provides a new PAC to a client after successful authentication when a configured percentage of the Tunnel PAC TTL remains. The server initiates the tunnel PAC update if the first successful authentication occurs before the PAC expires. This mechanism allows the client to be updated with a valid PAC. The default value is 10%.</td>
</tr>
<tr>
<td><strong>System will Assign SGT Numbers</strong></td>
<td>Choose this option if you want all the SGT numbers to be automatically generated by Cisco ISE.</td>
</tr>
<tr>
<td><strong>Except Numbers in Range</strong></td>
<td>Choose this option if you want to reserve a range of SGT numbers to be configured on the device manually. Cisco ISE will not use the values in this range while generating the SGTs.</td>
</tr>
<tr>
<td><strong>User Must Enter SGT Numbers Manually</strong></td>
<td>Choose this option to define the SGT numbers manually.</td>
</tr>
<tr>
<td><strong>Security Group Tag Numbering for APIC EPGs</strong></td>
<td>Check this check box and specify the range of numbers to be used for the SGTs created based on the EPGs learnt from APIC.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
</tr>
</tbody>
</table>
| **Auto Create Security Groups When Creating Authorization Rules** | Check this check box to create the SGTs automatically while creating the authorization policy rules.  
When this option is selected, the following message is displayed at the top of the Authorization Policy window: *Auto Security Group Creation is On*.  
The auto-created SGTs are named based on the rule attributes.  
**Note** The auto-created SGTs are not deleted when the corresponding authorization policy rule is deleted.  
By default, this option is disabled after a fresh install or upgrade. |
| **SGT Number Range For Auto-Creation** | Check this check box and specify the range of numbers to be used for the auto-created SGTs.  
When the range of numbers allocated for the auto-created SGTs are used up, Cisco ISE will extend the range by 50 and notify users about this change. |
| **Automatic Naming Options** | Use this option to define the naming convention for the auto-created SGTs.  
(Mandatory) **Name Will Include**—Choose one of the following options:  
- Rule name  
- SGT number  
- Rule name and SGT number  
By default, the Rule name option is selected.  
Optionally, you can add the following information to the SGT name:  
- Policy Set Name (this option is available only if Policy Sets are enabled)  
- Prefix (up to 8 characters)  
- Suffix (up to 8 characters)  
Cisco ISE will display a sample SGT name in the Example Name field based on your selections.  
If an SGT already exists with the same name, ISE will append _x to the SGT name, where x is the first value, starting at 1 (which is not in use in the current name).  
If the new name is longer than 32 characters, Cisco ISE will truncate it to the first 32 characters. |
Related Topics
- TrustSec Architecture, on page 807
- TrustSec Components, on page 808
- Configure TrustSec Global Settings, on page 814

TrustSec Matrix Settings

The following table describes the fields on the TrustSec Matrix Settings page. The navigation path for this page is: **Work Centers > TrustSec > Settings > TrustSec Matrix Settings**.

**Table 96: Configuring TrustSec Matrix Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow Multiple SGACLs</td>
<td>Check this check box if you want to allow multiple SGACLs in a cell. If this option is not selected, Cisco ISE will allow only one SGACL per cell. By default, this option is disabled upon fresh install. After upgrade, Cisco ISE will scan the Egress cells and if it identifies at least one cell with multiple SGACLs assigned to it, it allows the admin to add multiple SGACLs in a cell. Otherwise, it allows only one SGACL per cell. <strong>Note</strong> Before disabling multiple SGACLs, you must edit the cells containing multiple SGACLs to include only one SGACL.</td>
</tr>
<tr>
<td>Allow Monitoring</td>
<td>Check this check box to enable monitoring for all cells in the matrix. If monitoring is disabled, Monitor All icon is greyed out and the Monitor option is disabled in the Edit Cell dialog. By default, monitoring is disabled upon fresh install. <strong>Note</strong> Before disabling monitoring at matrix level, you must disable monitoring for the cells that are currently being monitored.</td>
</tr>
<tr>
<td>Show SGT Numbers</td>
<td>Use this option to display or hide the SGT values (both decimal and hexadecimal) in the matrix cells. By default, the SGT values are displayed in the cells.</td>
</tr>
</tbody>
</table>
| Appearance Settings        | The following options are available:  
  - Custom settings—The default theme (colors with no patterns) is displayed initially. You can set your own colors and patterns.  
  - Default settings—Predefined list of colors with no patterns (not editable).  
  - Accessibility settings—Predefined list of colors with patterns (not editable). |
Fields | Usage Guidelines
--- | ---
Color/Pattern | To make the matrix more readable, you can apply coloring and patterns to the matrix cells based on the cell contents. The following display types are available:
- Permit IP/Permit IP Log—Configured inside the cell
- Deny IP/Deny IP Log—Configured inside the cell
- SGACLs—For SGACLs configured inside the cell
- Permit IP/Permit IP Log (Inherited)—Taken from the default policy (for non-configured cells)
- Deny IP/Deny IP Log (Inherited)—Taken from the default policy (for non-configured cells)
- SGACLs (Inherited)—Taken from the default policy (for non-configured cells)

Related Topics
- Egress Policy, on page 823
- Matrix View, on page 824
- Configure TrustSec Matrix Settings, on page 815

**SMS Gateway Settings**

Use these settings to configure sending SMS messages to guests and sponsors via an email server.

*Table 97: SMS Gateway Settings for SMS Email Gateway*

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS Gateway Provider Domain</td>
<td>Enter the provider domain, which is used as the host portion and the guest account's mobile number as the user portion of the email address to send the message to the provider's SMS/MMS gateway.</td>
</tr>
</tbody>
</table>
| Provider account address | (Optional)

Enter the account address, which is used as the FROM address (typically the account address) for the email and overrides the Default Email Address global setting in Guest Access > Settings.
### Field: SMTP API destination address

**Usage Guidelines**

(Optional)

Enter the SMTP API Destination Address, if you are using an SMTP SMS API that requires a specific account recipient address, such as Clickatell SMTP API.

This is used as the TO address for the email and the guest account's mobile number is substituted into the message's body template.

### Field: SMTP API body template

**Usage Guidelines**

(Optional)

Enter the SMTP API Body Template, if you are using an SMTP SMS API that requires a specific email body template for sending the SMS, such as Clickatell SMTP API.

The supported dynamic substitutions are $mobilenumber$, $timestamp$ (of format $YYYYMMDDHHHMISSmimi$), and $message$. You can use $timestamp$ and $mobilenumber$ for SMS gateways that require a unique identifier in the URL.

The navigation path for these settings is **Guest Access > Settings > SMS Gateway**.

Use these settings to configure sending SMS messages to guests and sponsors via an HTTP API (GET or POST method).

#### Table 98: SMS Gateway Settings for SMS HTTP API

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
</table>
| **URL**                 | Enter the URL for the API. This field is not URL encoded. The guest account's mobile number is substituted into the URL. The supported dynamic substitutions are $mobilenumber$ and $message$.
|                         | If you are using HTTPS with the HTTP API, include HTTPS in the URL string and upload your provider's trusted certificates into Cisco ISE. Choose **Administration > System > Certificates > Trusted Certificates**. |
| **Data (Url encoded portion)** | Enter the Data (Url encoded portion) for the GET or POST request. This field is URL encoded. If using the default GET method, the data is appended to the URL specified above. |
### Usage Guidelines

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use HTTP POST method for data portion</td>
<td>If using the POST method, check this option. The data specified above is used as the content of the POST request.</td>
</tr>
<tr>
<td>HTTP POST data content type</td>
<td>If using the POST method, specify the content type such as &quot;plain/text&quot; or &quot;application/xml&quot;.</td>
</tr>
<tr>
<td>HTTPS Username</td>
<td>Enter this information.</td>
</tr>
<tr>
<td>HTTPS Password</td>
<td></td>
</tr>
<tr>
<td>HTTPS Host name</td>
<td></td>
</tr>
<tr>
<td>HTTPS Port number</td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics

- [SMS Providers and Services](#), on page 455
- [Configure SMS Gateways to Send SMS Notifications to Guests](#), on page 455

### DHCP and DNS Services

The navigation path for these settings is **Administration > System > Settings > DHCP & DNS Services**.

Use these settings to configure a DHCP, and optionally DNS, in order to enable Auth VLAN URL redirect simulation. You can create multiple scopes in order to apply them to different ISE nodes. If you apply multiple scopes to one ISE node, they should be configured on the same network interface.

---

**Note**

For Profiling, you may need a DHCP probe. ISE DHCP probe uses the same UDP port 67 as the Auth VLAN DHCP service. Therefore the DHCP probe should be configured on a different interface or can be disabled on this ISE node. For more information about DHCP probes, see [DHCP Probe](#), on page 647.

### Table 99: DHCP & DNS Service Settings for Auth VLAN URL Redirect Simulation

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope Name</td>
<td>Enter a name by which you can easily remember the purpose of this scope.</td>
</tr>
<tr>
<td>Status</td>
<td>Select <strong>Enabled</strong> or <strong>Disabled</strong>. The scope can only be used for an ISE node when enabled.</td>
</tr>
<tr>
<td>ISE Node</td>
<td>Apply an ISE node to act as the DHCP/DNS server. From the dropdown list, select the ISE node with which to use this scope. The Auth VLAN is defined per ISE node/network interface and no two interfaces or two nodes can share the same VLAN.</td>
</tr>
<tr>
<td>Field</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Network Interface</td>
<td>The network interfaces available for the ISE node that you selected appear in this dropdown list dynamically based on the ISE node that you selected. The Auth VLAN is defined per ISE node/network interface and no two interfaces or two nodes can share the same VLAN. Select the interface from which the DHCP/DNS server listens. Multiple VLANs may be connected to one network interface card by configuring a VLAN IP-helper on the NAD. For more information about configuring an IP helper, refer to the administration guide for the device for instructions.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>Enter the domain name for the DHCP server to be used in this scope.</td>
</tr>
<tr>
<td>DHCP Address range</td>
<td>Based on your network definitions, select the range of DHCP addresses available to be used for this scope.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>Based on your network definitions, select the network mask to be used for this scope.</td>
</tr>
<tr>
<td>Network ID</td>
<td>Automatically determined by Cisco ISE based on the DHCP attributes you enter.</td>
</tr>
<tr>
<td>Exclusion address range</td>
<td>Based on your network definitions, select the range of DHCP addresses that should not be used for this scope.</td>
</tr>
<tr>
<td>Default gateway</td>
<td>Enter the IP address of the default gateway.</td>
</tr>
<tr>
<td>DHCP lease time</td>
<td>Define the the DHCP lease time.</td>
</tr>
<tr>
<td>DHCP options</td>
<td>This is an optional field. DHCP options are added configuration parameters that a DHCP server can hand out to DHCP clients. DHCP options provide support for devices such as cameras, access points, or phones that require the information indicated in the option value in order to access the network, or as a method to bootstrap the device before final authorization. When the DHCP server receives the DHCP Request message from the client, the server (typically) responds by sending a DHCP ACK packet to the client. At this time, the server then forwards any configured options within the DHCP ACK packet. For more details, see the DHCP Options section below this table.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

If you would like users to be allowed access to external domains outside of the Auth VLAN before receiving authentication to access the entire corporate network, enter the IP addresses of the DNS servers to resolve the external DNS names.

**External DNS servers**

If you would like users to be allowed to access a specific site before receiving authentication to access the entire corporate network, enter the domain names of those sites in these fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>External DNS servers</td>
<td>If you would like users to be allowed access to external domains outside of the Auth VLAN before receiving authentication to access the entire corporate network, enter the IP addresses of the DNS servers to resolve the external DNS names.</td>
</tr>
<tr>
<td>External Domains</td>
<td>If you would like users to be allowed to access a specific site before receiving authentication to access the entire corporate network, enter the domain names of those sites in these fields.</td>
</tr>
</tbody>
</table>

### DHCP Options

When configuring a DHCP service in ISE, you can assign specific DHCP options for clients that connect to the Auth VLAN. You can add multiple DHCP options to each scope that you define.

The options available in the dropdown list are as taken from RFC 2132. You can also add additional customized options (from RFC 2132) by selecting **Custom** from the dropdown list and entering the option code.

In general, there are several DHCP options that tend to be used most frequently.

Common options include:

- Option 12 (Hostname)—used to carry the “hostname” portion of a node’s Fully Qualified Domain Name. For example, “mail” of mail.ise.com.
- Option 42 (NTP Servers)—carries the NTP servers used on the network.
- Option 66 (TFTP Server)—used to carry the IP address or hostname. This option is available in the dropdown list.
- Option 82 (DHCP Relay Agent)—used to carry other sub options for server side dhcp relay server information.

To define the option value, select an option from the dropdown list. The code and type populate automatically if you select a pre-defined **Option**.

If you select **Custom**, enter the **Code** and then the **Type** updates automatically. Enter the value of the option.
For example:

- To set a hostname—from **Option**, choose **Custom**. In **Code**, type 15. **Type** automatically updates to **Text**. In **Value**, type the hostname (such as "mail" of mail.ise.com).

- To set a TFTP Server Name—from **Option**, choose TFTP Server Name. **Code** and **Type** automatically update accordingly. In **Value**, type the TFTP server hostname.

---

**Note**

Some of the DHCP options cannot be manually entered because they are automatically defined for ISE. For example, Option 15 (Domain Name) cannot be defined as a custom option because the DHCP Domain name is already defined from this screen in a separate mandatory field and cannot be overridden.

To enter multiple options click the plus sign under **Actions**.

**Related Topics**

- Third-Party Network Device Support in Cisco ISE, on page 212
- Configure Third-Party Network Device in Cisco ISE, on page 216
- DHCP Probe, on page 647

---

**Identity Management**

These pages enable you to configure and manage identities in Cisco ISE.
Endpoints

These pages enable you to configure and manage endpoints that connect to your network.

Endpoint Settings

The following table describes the fields on the Endpoints page, which you can use to create endpoints and assign policies for endpoints. The navigation path for this page is: Work Centers > Network Access > Identities > Endpoints.

Table 100: Endpoint Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Enter the MAC address in hexadecimal format to create an endpoint statically. The MAC address is the device identifier for the interface that is connected to the Cisco ISE enabled network.</td>
</tr>
<tr>
<td>Static Assignment</td>
<td>Check this check box when you want to create an endpoint statically in the Endpoints page and the status of static assignment is set to static. You can toggle the status of static assignment of an endpoint from static to dynamic or from dynamic to static.</td>
</tr>
<tr>
<td>Policy Assignment</td>
<td>(Disabled by default unless the Static Assignment is checked) Choose a matching endpoint policy from the Policy Assignment drop-down list. You can do one of the following: • If you do not choose a matching endpoint policy, but use the default endpoint policy Unknown, then the static assignment status is set to dynamic for the endpoint that allows dynamic profiling of an endpoint. • If you choose a matching endpoint policy other than Unknown, then the static assignment status is set to static for that endpoint and the Static Assignment check box is automatically checked.</td>
</tr>
</tbody>
</table>
### Fields

<table>
<thead>
<tr>
<th>Static Group Assignment</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Disabled by default unless the Static group Assignment is checked) Check this check box when you want to assign an endpoint to an identity group statically. In you check this check box, the profiling service does not change the endpoint identity group the next time during evaluation of the endpoint policy for these endpoints, which were previously assigned dynamically to other endpoint identity groups. If you uncheck this check box, then the endpoint identity group is dynamic as assigned by the ISE profiler based on policy configuration. If you do not choose the Static Group Assignment option, then the endpoint is automatically assigned to the matching identity group the next time during evaluation of the endpoint policy.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identity Group Assignment</th>
<th>Choose an endpoint identity group to which you want to assign the endpoint. You can assign an endpoint to an identity group when you create an endpoint statically, or when you do not want to use the Create Matching Identity Group option during evaluation of the endpoint policy for an endpoint. Cisco ISE includes the following system created endpoint identity groups:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Blacklist</td>
<td>• Blacklist</td>
</tr>
<tr>
<td>• GuestEndpoints</td>
<td>• GuestEndpoints</td>
</tr>
<tr>
<td>• Profiled</td>
<td>• Profiled</td>
</tr>
<tr>
<td>• Cisco IP-Phone</td>
<td>• Cisco IP-Phone</td>
</tr>
<tr>
<td>• Workstation</td>
<td>• Workstation</td>
</tr>
<tr>
<td>• RegisteredDevices</td>
<td>• RegisteredDevices</td>
</tr>
<tr>
<td>• Unknown</td>
<td>• Unknown</td>
</tr>
</tbody>
</table>

### Related Topics

- Identified Endpoints, on page 711
- Create Endpoints with Static Assignments of Policies and Identity Groups, on page 707
Endpoint Import from LDAP Settings

The following table describes the fields on the Import from LDAP page, which you can use to import endpoints from an LDAP server. The navigation path for this page is: Work Centers > Network Access > Identities > Endpoints.

Table 101: Endpoint Import from LDAP Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connection Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Host</td>
<td>Enter the hostname, or the IP address of the LDAP server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number of the LDAP server. You can use the default port 389 to import from an LDAP server, and the default port 636 to import from an LDAP server over SSL.</td>
</tr>
<tr>
<td>Note</td>
<td>Cisco ISE supports any configured port number. The configured value should match the LDAP server connection details.</td>
</tr>
<tr>
<td>Enable Secure Connection</td>
<td>Check the Enable Secure Connection check box to import from an LDAP server over SSL.</td>
</tr>
<tr>
<td>Root CA Certificate Name</td>
<td>Click the drop-down arrow to view the trusted CA certificates.</td>
</tr>
<tr>
<td></td>
<td>The Root CA Certificate Name refers to the trusted CA certificate that is required to connect to an LDAP server. You can add (import), edit, delete, and export trusted CA certificates in Cisco ISE.</td>
</tr>
<tr>
<td>Anonymous Bind</td>
<td>Check the Anonymous Bind check box to enable the anonymous bind.</td>
</tr>
<tr>
<td></td>
<td>You must enable either the Anonymous Bind check box, or enter the LDAP administrator credentials from the slapd.conf configuration file.</td>
</tr>
<tr>
<td>Admin DN</td>
<td>Enter the distinguished name (DN) configured for the LDAP administrator in the slapd.conf configuration file.</td>
</tr>
<tr>
<td></td>
<td>Admin DN format example: cn=Admin, dc=cisco.com, dc=com</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password configured for the LDAP administrator in the slapd.conf configuration file.</td>
</tr>
<tr>
<td>Base DN</td>
<td>Enter the distinguished name of the parent entry.</td>
</tr>
<tr>
<td></td>
<td>Base DN format example: dc=cisco.com, dc=com</td>
</tr>
</tbody>
</table>
### Fields

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query Settings</td>
<td>Enter the query filter, which is used for importing the MAC address. For example, ieee802Device.</td>
</tr>
<tr>
<td>MAC Address objectClass</td>
<td>Enter the query filter, which is used for importing the MAC address. For example, ieee802Device.</td>
</tr>
<tr>
<td>MAC Address Attribute Name</td>
<td>Enter the returned attribute name for import. For example, macAddress.</td>
</tr>
</tbody>
</table>
| Profile Attribute Name         | Enter the name of the LDAP attribute. This attribute holds the policy name for each endpoint entry that is defined in the LDAP server. When you configure the Profile Attribute Name field, consider the following:  
  - If you do not specify this LDAP attribute in the Profile Attribute Name field or configure this attribute incorrectly, then endpoints are marked “Unknown” during an import operation, and these endpoints are profiled separately to the matching endpoint profiling policies.  
  - If you configure this LDAP attribute in the Profile Attribute Name field, the attribute values are validated to ensure that the endpoint policy matches with an existing policy in Cisco ISE, and endpoints are imported. If the endpoint policy does not match with an existing policy, then those endpoints will not be imported. |
| Time Out [seconds]             | Enter the time in seconds between 1 and 60 seconds.                               |

**Related Topics**
- Identified Endpoints, on page 711
- Import Endpoints from LDAP Server, on page 710

### Groups

These pages enable you to configure and manage endpoint identity groups.

### Endpoint Identity Group Settings

The following table describes the fields on the Endpoint Identity Groups page, which you can use to create an endpoint group. The navigation path for this page is: Administration > Identity Management > Groups > Endpoint Identity Groups.
Table 102: Endpoint Identity Group Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the endpoint identity group that you want to create.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the endpoint identity group that you want to create.</td>
</tr>
<tr>
<td>Parent Group</td>
<td>Choose an endpoint identity group from the Parent Group drop-down list to which you want to associate the newly created endpoint identity group.</td>
</tr>
</tbody>
</table>

Related Topics
- Identified Endpoints Grouped in Endpoint Identity Groups, on page 714
- Create Endpoint Identity Groups, on page 713

External Identity Sources

These pages enable you to configure and manage external identity sources that contain user data that Cisco ISE uses for authentication and authorization.

LDAP Identity Source Settings

The following table describes the fields on the LDAP Identity Sources page, which you can use to create an LDAP instance and connect to it. The navigation path for this page is: Administration > Identity Management > External Identity Sources > LDAP.

LDAP General Settings

The following table describes the fields in the General tab.

Table 103: LDAP General Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the LDAP instance. This value is used in searches to obtain the subject DN and attributes. The value is of type string and the maximum length is 64 characters.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the LDAP instance. This value is of type string, and has a maximum length of 1024 characters.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

You can choose any one of the following built-in schema types or create a custom schema:

- Active Directory
- Sun Directory Server
- Novell eDirectory

You can click the arrow next to Schema to view the schema details.

If you edit the attributes of the predefined schema, Cisco ISE automatically creates a Custom schema.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schema</td>
<td>You can choose any one of the following built-in schema types or create a custom schema:</td>
</tr>
<tr>
<td></td>
<td>• Active Directory</td>
</tr>
<tr>
<td></td>
<td>• Sun Directory Server</td>
</tr>
<tr>
<td></td>
<td>• Novell eDirectory</td>
</tr>
<tr>
<td></td>
<td>You can click the arrow next to Schema to view the schema details.</td>
</tr>
<tr>
<td></td>
<td>If you edit the attributes of the predefined schema, Cisco ISE automatically creates a</td>
</tr>
<tr>
<td></td>
<td>Custom schema.</td>
</tr>
</tbody>
</table>

**Note** The following fields can be edited only when you choose the Custom schema.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject Objectclass</td>
<td>Enter a value to be used in searches to obtain the subject DN and attributes. The value is of type string and the maximum length is 256 characters.</td>
</tr>
<tr>
<td>Subject Name Attribute</td>
<td>Enter the name of the attribute containing the username in the request. The value is of type string and the maximum length is 256 characters.</td>
</tr>
<tr>
<td>Group Name Attribute</td>
<td>Enter CN or DN or any supported attribute in the Group Name Attribute field.</td>
</tr>
<tr>
<td></td>
<td>• CN—To retrieve the LDAP Identity Store Groups based on Common Name.</td>
</tr>
<tr>
<td></td>
<td>• DN—To retrieve the LDAP Identity Store Groups based on Distinguished Name.</td>
</tr>
<tr>
<td>Certificate Attribute</td>
<td>Enter the attribute that contains the certificate definitions. For certificate-based authentication, these definitions are used to validate certificates that are presented by clients.</td>
</tr>
<tr>
<td>Group Objectclass</td>
<td>Enter a value to be used in searches to specify the objects that are recognized as groups. The value is of type string and the maximum length is 256 characters.</td>
</tr>
<tr>
<td>Group Map Attribute</td>
<td>Specifies the attribute that contains the mapping information. This attribute can be a user or group attribute based on the reference direction that is chosen.</td>
</tr>
<tr>
<td>Subject Objects Contain Reference To Groups</td>
<td>Click this radio button if the subject objects contain an attribute that specifies the group to which they belong.</td>
</tr>
</tbody>
</table>
**Fields** | **Usage Guidelines**
--- | ---
Group Objects Contain Reference To Subjects | Click this radio button if the group objects contain an attribute that specifies the subject. This value is the default value.

Subjects in Groups Are Stored in Member Attribute As | (Only available when you select the Group Objects Contain Reference To Subjects radio button) Specifies how members are sourced in the group member attribute and defaults to the DN.

User Info Attributes | By default, predefined attributes are used to collect user information (such as, first name, last name, email, telephone, locality, and so on) for the following built-in schema types:

  - Active Directory
  - Sun Directory Server
  - Novell eDirectory

If you edit the attributes of the predefined schema, Cisco ISE automatically creates a Custom schema. You can also select the Custom option from the Schema drop-down list to edit the user information attributes based on your requirements.

---

**LDAP Connection Settings**

The following table describes the fields in the Connection Settings tab.

*Table 104: LDAP Connection Settings*

| Fields | Usage Guidelines |
--- | --- |
Enable Secondary Server | Check this option to enable the secondary LDAP server to be used as a backup if the primary LDAP server fails. If you check this check box, you must enter configuration parameters for the secondary LDAP server. |

Primary and Secondary Servers

Hostname/IP | Enter the IP address or DNS name of the machine that is running the LDAP software. The hostname can contain from 1 to 256 characters or a valid IP address expressed as a string. The only valid characters for hostnames are alphanumeric characters (a to z, A to Z, 0 to 9), the dot (.), and the hyphen (-). |
<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Enter the TCP/IP port number on which the LDAP server is listening. Valid values are from 1 to 65,535. The default is 389, as stated in the LDAP specification. If you do not know the port number, you can find this information from the LDAP server administrator.</td>
</tr>
</tbody>
</table>
| Specify server for each ISE node | Check this checkbox to configure primary and secondary LDAP server hostnames/IP and their ports for each PSN.  
When this option is enabled, a table listing all the nodes in the deployment is displayed. You need to select the node and configure the primary and secondary LDAP server hostname/IP and their ports for the selected node. |
| Access                       | Anonymous Access—Click to ensure that searches on the LDAP directory occur anonymously. The server does not distinguish who the client is and will allow the client read access to any data that is configured as accessible to any unauthenticated client. In the absence of a specific policy permitting authentication information to be sent to a server, a client should use an anonymous connection.  
Authenticated Access—Click to ensure that searches on the LDAP directory occur with administrative credentials. If so, enter information for the Admin DN and Password fields. |
<p>| Admin DN                     | Enter the DN of the administrator. The Admin DN is the LDAP account that has permission to search all required users under the User Directory Subtree and to search groups. If the administrator specified does not have permission to see the group name attribute in searches, group mapping fails for users who are authenticated by that LDAP server. |
| Password                     | Enter the LDAP administrator account password.                                                                                                                                                        |
| Secure Authentication        | Click to use SSL to encrypt communication between Cisco ISE and the primary LDAP server. Verify that the Port field contains the port number used for SSL on the LDAP server. If you enable this option, you must choose a root CA. |
| LDAP Server Root CA          | Choose a trusted root certificate authority from the drop-down list to enable secure authentication with a certificate.                                                                                   |</p>
<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Timeout</td>
<td>Enter the number of seconds that Cisco ISE waits for a response from the primary LDAP server before determining that the connection or authentication with that server has failed. Valid values are 1 to 99. The default is 10.</td>
</tr>
<tr>
<td>Max. Admin Connections</td>
<td>Enter the maximum number of concurrent connections (greater than 0) with LDAP administrator account permissions that can run for a specific LDAP configuration. These connections are used to search the directory for users and groups under the User Directory Subtree and the Group Directory Subtree. Valid values are 1 to 99. The default is 20.</td>
</tr>
<tr>
<td>Force reconnect every N seconds</td>
<td>Check this check box and enter the desired value in the Seconds text box to force the server to renew LDAP connection at the specified time interval. The valid range is from 1 to 60 minutes.</td>
</tr>
<tr>
<td>Test Bind to Server</td>
<td>Click to test and ensure that the LDAP server details and credentials can successfully bind. If the test fails, edit your LDAP server details and retest.</td>
</tr>
<tr>
<td>Failover</td>
<td></td>
</tr>
<tr>
<td>Always Access Primary Server First</td>
<td>Click this option if you want Cisco ISE to always access the primary LDAP server first for authentications and authorizations.</td>
</tr>
<tr>
<td>Failback to Primary Server After</td>
<td>If the primary LDAP server that Cisco ISE attempts to contact cannot be reached, Cisco ISE attempts to contact the secondary LDAP server. If you want Cisco ISE to use the primary LDAP server again, click this option and enter a value in the text box.</td>
</tr>
</tbody>
</table>

**LDAP Directory Organization Settings**

The following table describes the fields in the Directory Organization tab.
Table 105: LDAP Directory Organization Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject Search Base</td>
<td>Enter the DN for the subtree that contains all subjects. For example: o=corporation.com If the tree containing subjects is the base DN, enter: o=corporation.com or dc=corporation,dc=com as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.</td>
</tr>
<tr>
<td>Group Search Base</td>
<td>Enter the DN for the subtree that contains all groups. For example: ou=organizational unit, ou=next organizational unit, o=corporation.com If the tree containing groups is the base DN, type: o=corporation.com or dc=corporation,dc=com as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Search for MAC Address in Format                | Enter a MAC Address format for Cisco ISE to use for search in the LDAP database. MAC addresses in internal identity sources are sourced in the format `xx-xx-xx-xx-xx-xx`. MAC addresses in LDAP databases can be sourced in different formats. However, when Cisco ISE receives a host lookup request, Cisco ISE converts the MAC address from the internal format to the format that is specified in this field. Use the drop-down list to enable searching for MAC addresses in a specific format, where `<format>` can be any one of the following:  
  - `xxxx.xxxx.xxxx`  
  - `xxxxxxxxxxxx`  
  - `xx-xx-xx-xx-xx-xx`  
The format you choose must match the format of the MAC address sourced in the LDAP server. |
| Strip Start of Subject Name Up To the Last Occurrence of the Separator | Enter the appropriate text to remove domain prefixes from usernames. If, in the username, Cisco ISE finds the delimiter character that is specified in this field, it strips all characters from the beginning of the username through the delimiter character. If the username contains more than one of the characters that are specified in the `<start_string>` box, Cisco ISE strips characters through the last occurrence of the delimiter character. For example, if the delimiter character is the backslash (\) and the username is `DOMAIN\user1`, Cisco ISE submits `user1` to an LDAP server. **Note** The `<start_string>` cannot contain the following special characters: the pound sign (#), the question mark (?), the quotation mark ("), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). Cisco ISE does not allow these characters in usernames. |
### Usage Guidelines

#### Fields

**Strip End of Subject Name from the First Occurrence of the Separator**

Enter the appropriate text to remove domain suffixes from usernames.

If, in the username, Cisco ISE finds the delimiter character that is specified in this field, it strips all characters from the delimiter character through the end of the username. If the username contains more than one of the characters that are specified in this field, Cisco ISE strips characters starting with the first occurrence of the delimiter character. For example, if the delimiter character is `@` and the username is `user1@domain`, then Cisco ISE submits `user1` to the LDAP server.

**Note**
The `<end_string>` box cannot contain the following special characters: the pound sign (`#`), the question mark (`?`), the quotation mark (`"`), the asterisk (`*`), the right angle bracket (`>`, and the left angle bracket (`<`). Cisco ISE does not allow these characters in usernames.

### LDAP Group Settings

**Table 106: LDAP Group Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Add</strong></td>
<td>Choose <strong>Add &gt; Add Group</strong> to add a new group or choose <strong>Add &gt; Select Groups From Directory</strong> to select the groups from the LDAP directory.</td>
</tr>
<tr>
<td></td>
<td>If you choose to add a group, enter a name for the new group. If you are selecting from the directory, enter the filter criteria, and click <strong>Retrieve Groups</strong>. Check the check boxes next to the groups that you want to select and click OK. The groups that you have selected will appear in the Groups page.</td>
</tr>
</tbody>
</table>
### LDAP Attribute Settings

**Table 107: LDAP Attribute Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Choose <strong>Add &gt; Add Attribute</strong> to add a new attribute or choose <strong>Add &gt; Select Attributes From Directory</strong> to select attributes from the LDAP server. If you choose to add an attribute, enter a name for the new attribute. If you are selecting from the directory, enter the username and click <strong>Retrieve Attributes</strong> to retrieve the user’s attributes. Check the checkboxes next to the attributes that you want to select, and then click OK.</td>
</tr>
</tbody>
</table>

### LDAP Advanced Settings

The following table describes the field in the Advanced Settings tab.

**Table 108: LDAP Advanced Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Password Change</td>
<td>Check this check box to enable the user to change the password in case of password expiry or password reset while using PAP protocol for device admin and RADIUS EAP-GTC protocol for network access. User authentication fails for the unsupported protocols. This option also enables the user to change the password on their next login.</td>
</tr>
</tbody>
</table>

### Related Topics

- [LDAP Directory Service](#), on page 409
- [LDAP User Authentication](#), on page 410
- [LDAP User Lookup](#), on page 413
- [Add LDAP Identity Sources](#), on page 414

### RADIUS Token Identity Sources Settings

The following table describes the fields on the RADIUS Token Identity Sources page, which you can use to configure and connect to an external RADIUS identity source. The navigation path for this page is: Administration > Identity Management > External Identity Sources > RADIUS Token.

**Table 109: RADIUS Token Identity Source Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the RADIUS token server. The maximum number of characters allowed is 64.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the RADIUS token server. The maximum number of characters is 1024.</td>
</tr>
<tr>
<td>SafeWord Server</td>
<td>Check this check box if your RADIUS identity source is a SafeWord server.</td>
</tr>
<tr>
<td>Enable Secondary Server</td>
<td>Check this check box to enable the secondary RADIUS token server for Cisco ISE to use as a backup in case the primary fails. If you check this check box, you must configure a secondary RADIUS token server.</td>
</tr>
<tr>
<td>Always Access Primary Server First</td>
<td>Click this radio button if you want Cisco ISE to always access the primary server first.</td>
</tr>
<tr>
<td>Fallback to Primary Server after</td>
<td>Click this radio button to specify the amount of time in minutes that Cisco ISE can authenticate using the secondary RADIUS token server if the primary server cannot be reached. After this time elapses, Cisco ISE reattempts to authenticate against the primary server.</td>
</tr>
</tbody>
</table>

**Primary Server**

<table>
<thead>
<tr>
<th>Host IP</th>
<th>Enter the IP address of the primary RADIUS token server. This field can take as input a valid IP address that is expressed as a string. Valid characters that are allowed in this field are numbers and dot (.).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret that is configured on the primary RADIUS token server for this connection.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>Enter the port number on which the primary RADIUS token server is listening. Valid values are from 1 to 65,535. The default is 1812.</td>
</tr>
<tr>
<td>Server Timeout</td>
<td>Specify the time in seconds that Cisco ISE should wait for a response from the primary RADIUS token server before it determines that the primary server is down. Valid values are 1 to 300. The default is 5.</td>
</tr>
<tr>
<td>Connection Attempts</td>
<td>Specify the number of attempts that Cisco ISE should make to reconnect to the primary server before moving on to the secondary server (if defined) or dropping the request if a secondary server is not defined. Valid values are 1 to 9. The default is 3.</td>
</tr>
</tbody>
</table>

**Secondary Server**

<table>
<thead>
<tr>
<th>Host IP</th>
<th>Enter the IP address of the secondary RADIUS token server. This field can take as input a valid IP address that is expressed as a string. Valid characters that are allowed in this field are numbers and dot (.).</th>
</tr>
</thead>
</table>
### RSA SecurID Identity Source Settings

The following table describes the fields on the RSA SecurID Identity Sources page, which you can use to create and connect to an RSA SecurID identity source. The navigation path for this page is: **Administration > Identity Management > External Identity Sources > RSA SecurID.**

#### RSA Prompt Settings

The following table describes the fields in the RSA Prompts tab.

**Table 110: RSA Prompt Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Passcode Prompt</td>
<td>Enter a text string to obtain the passcode.</td>
</tr>
<tr>
<td>Enter Next Token Code</td>
<td>Enter a text string to request the next token.</td>
</tr>
<tr>
<td>Choose PIN Type</td>
<td>Enter a text string to request the PIN type.</td>
</tr>
<tr>
<td>Accept System PIN</td>
<td>Enter a text string to accept the system-generated PIN.</td>
</tr>
<tr>
<td>Enter Alphanumeric PIN</td>
<td>Enter a text string to request an alphanumeric PIN.</td>
</tr>
<tr>
<td>Enter Numeric PIN</td>
<td>Enter a text string to request a numeric PIN.</td>
</tr>
<tr>
<td>Re-enter PIN</td>
<td>Enter a text string to request the user to re-enter the PIN.</td>
</tr>
</tbody>
</table>
**RSA Message Settings**

The following table describes the fields in the RSA Messages tab.

*Table 111: RSA Messages Settings*

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display System PIN Message</td>
<td>Enter a text string to label the system PIN message.</td>
</tr>
<tr>
<td>Display System PIN Reminder</td>
<td>Enter a text string to inform the user to remember the new PIN.</td>
</tr>
<tr>
<td>Must Enter Numeric Error</td>
<td>Enter a message that instructs users to enter only numbers for the PIN.</td>
</tr>
<tr>
<td>Must Enter Alpha Error</td>
<td>Enter a message that instructs users to enter only alphanumeric characters for PINs.</td>
</tr>
<tr>
<td>PIN Accepted Message</td>
<td>Enter a message that the users see when their PIN is accepted by the system.</td>
</tr>
<tr>
<td>PIN Rejected Message</td>
<td>Enter a message that the users see when the system rejects their PIN.</td>
</tr>
<tr>
<td>User Pins Differ Error</td>
<td>Enter a message that the users see when they enter an incorrect PIN.</td>
</tr>
<tr>
<td>System PIN Accepted Message</td>
<td>Enter a message that the users see when the system accepts their PIN.</td>
</tr>
<tr>
<td>Bad Password Length Error</td>
<td>Enter a message that the users see when the PIN that they specify does not fall within the range specified in the PIN length policy.</td>
</tr>
</tbody>
</table>

**Related Topics**
- RSA Identity Sources, on page 428
- Cisco ISE and RSA SecurID Server Integration, on page 428
- Add RSA Identity Sources, on page 430

**Identity Management Settings**

**User Authentication Policy Settings**

The following table describes the fields in the User Authentication Settings page, which you can use to define a criteria for user passwords and to disable admin and network access user accounts. The navigation path for this page is: **Administration > Identity Management > Settings > User Authentication Settings**.

*Table 112: User Password Policy Settings*

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Length</td>
<td>Sets the minimum length of password (in characters)</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Username</td>
<td>Restricts the use of the username or its characters in reversed order</td>
</tr>
<tr>
<td>Cisco</td>
<td>Restricts the use of “cisco” or its characters in reversed order</td>
</tr>
<tr>
<td>Special characters</td>
<td>Restricts the use of special characters that you define in reverse order</td>
</tr>
<tr>
<td>Repeated characters</td>
<td>Restricts the use of characters repeated four or more times consecutively</td>
</tr>
<tr>
<td>Required characters</td>
<td>Requires that the password includes at least one of each of the following types: • Lowercase alphabetic characters • Uppercase alphabetic characters • Numeric characters • Non-alphanumeric characters</td>
</tr>
<tr>
<td>Password History</td>
<td>Enter the number of previous versions from which the password must be different to prevent the repeated use of the same password You can also enter the number of characters that must be different from the previous password Enter the number of days before which you cannot reuse a password</td>
</tr>
<tr>
<td>Password Lifetime</td>
<td>Sets the following options to force users to change passwords after a specified time period: • Time (in days) before the user account is disabled if the password is not changed • Reminder (in days) before the user account is disabled</td>
</tr>
<tr>
<td>Lock or Suspend Account with Incorrect Login Attempts</td>
<td>Specifies the number of times Cisco ISE records incorrect administrator passwords before locking the administrator out of Cisco ISE, and suspending or disabling account credentials. An e-mail is sent to the administrator whose account gets locked out. You can enter a custom e-mail remediation message.</td>
</tr>
</tbody>
</table>
Account Display Policy

While authenticating or querying a user, Cisco ISE checks the global account disable policy settings (Administration > Identity Management > Settings > User Authentication Settings):

- Disable user accounts that exceed a specified date (yyyy-mm-dd). However, the account disable policy settings for a particular network access user (Administration > Identity Management > Identities > Users > Account Disable Policy) takes precedence over the global settings.

- Disable user accounts that exceed the specified number of days from when the user account was created or the last date when the user was enabled (Administration > Identity Management > Identities > Users > Status).

- Disable admin and user accounts that have not been authenticated for a consecutive number of days.

The account disable policy settings specified for a network access user in Cisco Secure ACS is migrated to Cisco ISE.

Related Topics
- User Account Custom Attributes and Password Policies, on page 310
- Add Users, on page 313

Network Resources

Network Devices

These pages enable you to add and manage network devices.

Network Device Definition Settings

The following table describes the fields in the Network Devices page, which you can use to configure a network access device in Cisco ISE. The navigation path for this page is: Administration > Network Resources > Network Devices.

Network Device Settings

The following table describes the fields in the Network Device section.

Table 113: Network Device Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name for the network device. You can provide a descriptive name to the network device that can be different from the hostname of the device. The device name is a logical identifier. Note: You cannot edit the name of a device once configured.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description for the device.</td>
</tr>
</tbody>
</table>
Choose one of the following:

- **IP Address**—Enter a single IP address (IPv4 or IPv6 address) and a subnet mask.
- **IP Ranges**—Enter the required IPv4 address range. You can also enter an IP address or IP address range in the Exclude text box to exclude IP addresses during authentication.

The following are the guidelines that must be followed while defining the IP addresses and subnet masks or IP address ranges:

- You can define a specific IP address, or a range with a subnet mask. If device A has an IP address range defined, you can configure another device B with an individual address from the range that is defined in device A.
- You can define IP address ranges in all the octets. You can use a hyphen (-) or use asterisk (*) as wildcard to specify a range of IP addresses. For example, *.*.*.*, 1-10.1-10.1-10 or 10-11.*.5.10-15.
- You can exclude a subset of IP address range from the configured range in a scenario where that subset has already been added. For example, 10.197.65.*/10.197.65.1 or 10.197.65.* exclude 10.197.65.1.
- You cannot define two devices with the same specific IP addresses.
- You cannot define two devices with the same IP range. The IP ranges must not overlap either partially or completely.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Type</strong></td>
<td>Click the drop-down list to select the vendor of the network device. You can use the tooltip next to the drop-down list to see the flows and services that the selected vendor's network devices support, as well as the RADIUS CoA port and type of URL redirect used by the device. These attributes are defined in the device type's network device profile.</td>
</tr>
</tbody>
</table>
Network Device Definition Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Name</td>
<td>Click the drop-down list to choose the device model, for example. You can use the model name as one of the parameters while checking for conditions in rule-based policies. This attribute is present in the device dictionary.</td>
</tr>
<tr>
<td>Software Version</td>
<td>Click the drop-down list to choose the version of the software running on the network device. You can use the software version as one of the parameters while checking for conditions in rule-based policies. This attribute is present in the device dictionary.</td>
</tr>
<tr>
<td>Network Device Group</td>
<td>Click the Location and Device Type drop-down lists to choose a location and device type that can be associated with the network device. If you do not specifically assign a device to a group when you configure it, it becomes a part of the default device groups (root NDGs), which is All Locations by location and All Device Types by device type and the default device groups (root NDGs) are assigned. For example, All Locations and All Device Groups.</td>
</tr>
</tbody>
</table>

RADIUS Authentication Settings

The following table describes the fields in the RADIUS Authentication Settings section.

Table 114: RADIUS Authentication Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS UDP Settings</td>
<td>Displays RADIUS as the selected protocol.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret for the network device. The shared secret is the key that you have configured on the network device using the radius-host command with the pac option. Note: Shared secret length must be equal to or greater than the value configured in the Minimum RADIUS Shared Secret Length field in the Device Security Settings page (Administration &gt; Network Resources &gt; Network Devices &gt; Device Security Settings). For the RADIUS server, best practice is to have 22 characters. Note that for new installation and upgraded deployment, by default, this value is 4 characters. You can change this value on the Device Security Settings page.</td>
</tr>
<tr>
<td>CoA Port</td>
<td>Specify the port to be used for RADIUS CoA. The default CoA port for the device is defined in the network device profile. Note: If you modify the CoA port specified in the Network Devices page (Administration &gt; Network Resources &gt; Network Devices) under RADIUS Authentication Settings, make sure that you specify the same CoA port for the corresponding profile in the Network Device Profile page (Administration &gt; Network Resources &gt; Network Device Profiles).</td>
</tr>
<tr>
<td>RADIUS DTLS Settings</td>
<td>If you enable this option, Cisco ISE will process only the DTLS requests from this device. If this option is disabled, Cisco ISE will process both UDP and DTLS requests from this device. RADIUS DTLS provides improved security for SSL tunnel establishment and RADIUS communication.</td>
</tr>
<tr>
<td>DTLS Required</td>
<td>Displays the shared secret used for RADIUS DTLS. This value is fixed and used to compute the MD5 integrity checks.</td>
</tr>
<tr>
<td>CoA Port</td>
<td>Specify the port to be used for RADIUS DTLS CoA.</td>
</tr>
</tbody>
</table>
### Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Issuer CA of ISE Certificates for CoA</strong></td>
<td>Select the Certificate Authority to be used for RADIUS DTLS CoA from the drop-down list.</td>
</tr>
<tr>
<td><strong>DNS Name</strong></td>
<td>Enter the DNS name of the network device. If the <strong>Enable RADIUS/DTLS Client Identity Verification</strong> option is enabled under RADIUS settings, Cisco ISE compares this DNS name with the DNS name that is specified in the client certificate to verify the identity of the network device.</td>
</tr>
</tbody>
</table>

**General Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable KeyWrap</strong></td>
<td>Check this check box only when supported on the network device, which increases RADIUS security via an AES KeyWrap algorithm.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When you run Cisco ISE in FIPS mode, you must enable KeyWrap on the network device.</td>
</tr>
<tr>
<td><strong>Key Encryption Key</strong></td>
<td>(Only appears when you enable KeyWrap) Enter an encryption key that is used for session encryption (secrecy).</td>
</tr>
<tr>
<td><strong>Message Authenticator Code Key</strong></td>
<td>(Only appears when you enable KeyWrap) Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages.</td>
</tr>
<tr>
<td><strong>Key Input Format</strong></td>
<td>Choose one of the following formats:</td>
</tr>
<tr>
<td></td>
<td>• <strong>ASCII</strong>—The Key Encryption Key must be 16 characters (bytes) long, and the Message Authenticator Code Key must be 20 characters (bytes) long.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hexadecimal</strong>—The Key Encryption Key must be 32 bytes long, and the Message Authenticator Code Key must be 40 bytes long.</td>
</tr>
</tbody>
</table>

**TACACS+ Authentication Settings**

The following table describes the fields on the Network Devices page, which you can use to configure TACACS+ authentication settings for a network device. The navigation path is:
• (For Network Devices) **Work Centers > Device Administration > Network Resources > Network Devices > Add > TACACS Authentication Settings.**

• (For Default Devices) **Work Centers > Device Administration > Network Resources > Default Devices > TACACS Authentication Settings.** You can refer to the Default Network Device Definition in Cisco ISE section for more information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared Secret</td>
<td>A string of text assigned to a network device when TACACS+ protocol is enabled. A user must enter the text before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret. This is not a mandatory field.</td>
</tr>
<tr>
<td>Retired Shared Secret is Active</td>
<td>Displayed when the retirement period is active.</td>
</tr>
<tr>
<td>Retire</td>
<td>Retires an existing shared secret instead of ending it. When you click Retire, a message box is displayed. You can either click Yes or No.</td>
</tr>
<tr>
<td>Remaining Retired Period</td>
<td>(Available only if you select Yes in the above message box) Displays the default value specified in the following navigation path: <strong>Work Centers &gt; Device Administration &gt; Settings &gt; Connection Settings &gt; Default Shared Secret Retirement Period.</strong> You can change the default values. This allows a new shared secret to be entered and the old shared secret will remain active for the specified number of days.</td>
</tr>
<tr>
<td>End</td>
<td>(Available only if you select Yes in the above message box) Ends the retirement period and terminates the old shared secret.</td>
</tr>
</tbody>
</table>
| Enable Single Connect Mode | Check to use a single TCP connection for all TACACS+ communication with the network device. Choose one of the following:  
  • Legacy Cisco Devices  
  • Or, TACACS+ Draft Compliance Single Connect Support. If you disable Single Connect Mode, ISE uses a new TCP connection for every TACACS+ request. |

**SNMP Settings**

The following table describes the fields in the SNMP Settings section.
### Table 115: SNMP Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Version</td>
<td>Choose an SNMP version from the Version drop-down list to be used for requests. Version includes the following:</td>
</tr>
<tr>
<td></td>
<td>• 1—SNMPv1 does not support informs.</td>
</tr>
<tr>
<td></td>
<td>• 2c</td>
</tr>
<tr>
<td></td>
<td>• 3—SNMPv3 is the most secure model because it allows packet encryption when you choose the Priv security level.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you have configured your network device with SNMPv3 parameters, you cannot generate the Network Device Session Status Summary report that is provided by the Monitoring service (Operations &gt; Reports &gt; Catalog &gt; Network Device &gt; Session Status Summary). You can generate this report successfully if your network device is configured with SNMPv1 or SNMPv2c parameters.</td>
</tr>
<tr>
<td>SNMP RO Community</td>
<td>(Only for SNMP Versions 1 and 2c when selected) Enter the Read Only Community string that provides Cisco ISE with a particular type of access to the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The caret (circumflex <code>^</code>) symbol is not allowed to be used.</td>
</tr>
<tr>
<td>SNMP Username</td>
<td>(Only for SNMP Version 3) Enter SNMP username.</td>
</tr>
<tr>
<td>Security Level</td>
<td>(Only for SNMP Version 3) Choose the security level from the following:</td>
</tr>
<tr>
<td></td>
<td>• Auth—Enables Message Digest 5 or Secure Hash Algorithm (SHA) packet authentication</td>
</tr>
<tr>
<td></td>
<td>• No Auth—No authentication and no privacy security level</td>
</tr>
<tr>
<td></td>
<td>• Priv—Enables Data Encryption Standard (DES) packet encryption</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Auth Protocol</td>
<td>(Only for SNMP Version 3 when the security levels Auth and Priv are selected) Choose the authentication protocol that you want the network device to use.</td>
</tr>
<tr>
<td></td>
<td>Authentication Protocol includes one of the following for security levels of Auth and Priv:</td>
</tr>
<tr>
<td></td>
<td>• MD5</td>
</tr>
<tr>
<td></td>
<td>• SHA</td>
</tr>
<tr>
<td>Auth Password</td>
<td>(Only for SNMP Version 3 when the security levels Auth and Priv are selected) Enter the authentication key that must be at least 8 characters in length.</td>
</tr>
<tr>
<td></td>
<td>Click Show to display the Auth Password that is already configured for the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The caret (^) symbol is not allowed to be used in the password.</td>
</tr>
<tr>
<td>Privacy Protocol</td>
<td>(Only for SNMP Version 3 when the security level Priv is selected) Choose the privacy protocol that you want the network device to use.</td>
</tr>
<tr>
<td></td>
<td>Privacy Protocols are one of the following:</td>
</tr>
<tr>
<td></td>
<td>• DES</td>
</tr>
<tr>
<td></td>
<td>• AES128</td>
</tr>
<tr>
<td></td>
<td>• AES192</td>
</tr>
<tr>
<td></td>
<td>• AES256</td>
</tr>
<tr>
<td></td>
<td>• 3DES</td>
</tr>
<tr>
<td>Privacy Password</td>
<td>(Only for SNMP Version 3 when the security level Priv is selected) Enter the privacy key.</td>
</tr>
<tr>
<td></td>
<td>Click Show to display the Privacy Password that is already configured for the device.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The caret (^) symbol is not allowed to be used in the password.</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Enter the polling interval in seconds. The default is 3600 seconds.</td>
</tr>
<tr>
<td>Link Trap Query</td>
<td>Check this check box to receive and interpret linkup and linkdown notifications received through the SNMP Trap.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mac Trap Query</td>
<td>Check this check box to receive and interpret MAC notifications received through the SNMP Trap</td>
</tr>
<tr>
<td>Originating Policy Service Node</td>
<td>Indicates which ISE server to be used to poll for SNMP data. By default, it is automatic, but you can overwrite the setting by assigning different values.</td>
</tr>
</tbody>
</table>

**Advanced TrustSec Settings**

The following table describes the fields in the **Advanced TrustSec Settings** section.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TrustSec Device Notification and Updates Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Use Device ID for TrustSec Identification</td>
<td>Check this check box if you want the device name to be listed as the device identifier in the Device ID field.</td>
</tr>
<tr>
<td>Device ID</td>
<td>You can enter the device ID in this field only if you have not checked the Use Device ID for TrustSec Identification check box.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password that you have configured on the TrustSec device CLI to authenticate the TrustSec device. Click <strong>Show</strong> to display the password that is used to authenticate the TrustSec device.</td>
</tr>
<tr>
<td>Download Environment Data Every &lt;...&gt;</td>
<td>Specify the time interval at which the device must download its environment data from Cisco ISE. You can specify the time in seconds, minutes, hours, weeks, or days. The default value is 1 day.</td>
</tr>
<tr>
<td>Download Peer Authorization Policy Every &lt;...&gt;</td>
<td>Specify the time interval at which the device must download the peer authorization policy from Cisco ISE. You can specify the time in seconds, minutes, hours, weeks, or days. The default value is 1 day.</td>
</tr>
<tr>
<td>Reauthentication Every &lt;...&gt;</td>
<td>Specify the time interval at which the device re authenticates itself against Cisco ISE after the initial authentication. You can configure the time interval in seconds, minutes, hours, weeks or days. For example, if you enter 1000 seconds, the device will authenticate itself against Cisco ISE every 1000 seconds. The default value is 1 day.</td>
</tr>
</tbody>
</table>
**Fields** | **Usage Guidelines**
---|---
**Download SGACL Lists Every <...>** | Specify the time interval at which the device downloads SGACL lists from Cisco ISE. You can configure the time interval in seconds, minutes, hours, weeks or days. The default value is 1 day.

**Other TrustSec Devices to Trust This Device (TrustSec Trusted)** | Check this check box if you want all the peer devices to trust this TrustSec device. If you uncheck this check box, the peer devices do not trust this device, and all the packets that arrive from this device are colored or tagged accordingly.

**Notify this device about TrustSec configuration changes** | Check this check box if you want Cisco ISE to send TrustSec CoA notifications to this TrustSec device.

**Device Configuration Deployment Settings**

**Include this device when deploying Security Group Tag Mapping Updates** | Check this check box if you want the TrustSec device to obtain the IP-SGT mappings using device interface credentials.

**EXEC Mode Username** | Enter the username that you use to log in to the TrustSec device.

**EXEC Mode Password** | Enter the device password.

**Enable Mode Password** | (Optional) Enter the enable password that is used to edit the configuration of the TrustSec device in privileged mode.

**Out Of Band TrustSec PAC Display**

**Issue Date** | Displays the issuing date of the last TrustSec PAC that has been generated by Cisco ISE for the TrustSec device.

**Expiration Date** | Displays the expiration date of the last TrustSec PAC that has been generated by Cisco ISE for the TrustSec device.

**Issued By** | Displays the name of the issuer (a TrustSec administrator) of the last TrustSec PAC that has been generated by Cisco ISE for the TrustSec device.

**Generate PAC** | Click this option to generate the out-of-band TrustSec PAC for the TrustSec device.

**Related Topics**

- [Network Devices Definitions in Cisco ISE](#), on page 209
- [Third-Party Network Device Support in Cisco ISE](#), on page 212
- [Network Device Groups](#), on page 219
- [Create a Network Device Definition in Cisco ISE](#), on page 188
Configure Third-Party Network Device in Cisco ISE, on page 216

Default Network Device Definition Settings

The following table describes the fields in the Default Network device page, which allows you to configure a default network device that Cisco ISE can use for RADIUS or TACACS+ authentication. Choose one of the navigation paths:

- Administration > Network Resources > Network Devices > Default Device
- Work Centers > Device Administration > Network Resources > Default Devices

Table 117: Default Network Device Definition Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Network Device Status</td>
<td>Choose Enable from the Default Network Device Status drop-down list to enable the default network device definition.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If the default device is enabled, you must enable either RADIUS or TACACS+ authentication settings.</td>
</tr>
<tr>
<td>Device Profile</td>
<td>Displays Cisco as the default device vendor.</td>
</tr>
<tr>
<td>RADIUS Authentication Settings</td>
<td></td>
</tr>
<tr>
<td>Enable RADIUS</td>
<td>Check this check box if you want to enable RADIUS authentication for the device.</td>
</tr>
<tr>
<td>RADIUS UDP Settings</td>
<td></td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter a shared secret. The shared secret can be up to 127 characters in length.</td>
</tr>
<tr>
<td></td>
<td>The shared secret is the key that you have configured on the network device using the <code>radius-host</code> command with the <code>pac</code> option.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Shared secret length must be equal to or greater than the value configured in the Minimum RADIUS Shared Secret Length field in the Device Security Settings page (Administration &gt; Network Resources &gt; Network Devices &gt; Device Security Settings). By default, this value is 4 characters for new installation and upgraded deployment. For the RADIUS server, best practice is to have 22 characters.</td>
</tr>
<tr>
<td>RADIUS DTLS Settings</td>
<td></td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>DTLS Required</td>
<td>If you enable this option, Cisco ISE will process only the DTLS requests from this device. If this option is disabled, Cisco ISE will process both UDP and DTLS requests from this device. RADIUS DTLS provides improved security for SSL tunnel establishment and RADIUS communication.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Displays the shared secret used for RADIUS DTLS. This value is fixed and is used to compute the MD5 integrity checks.</td>
</tr>
<tr>
<td>Issuer CA of ISE Certificates for CoA</td>
<td>Select the Certificate Authority to be used for RADIUS DTLS CoA from the drop-down list.</td>
</tr>
<tr>
<td><strong>General Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Enable KeyWrap</td>
<td>Check this check box only when supported on the network device, which increases RADIUS security via an AES KeyWrap algorithm. When you run Cisco ISE in FIPS mode, you must enable KeyWrap on the network device.</td>
</tr>
<tr>
<td>Key Encryption Key</td>
<td>Enter an encryption key that is used for session encryption (secrecy) when you enable KeyWrap.</td>
</tr>
<tr>
<td>Message Authenticator Code Key</td>
<td>Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages when you enable KeyWrap.</td>
</tr>
</tbody>
</table>
| Key Input Format                     | Choose one of the following formats:  
  - **ASCII**—The Key Encryption Key must be 16 characters (bytes) long, and the Message Authenticator Code Key must be 20 characters (bytes) long.  
  - **Hexadecimal**—The Key Encryption Key must be 32 bytes long, and the Message Authenticator Code Key must be 40 bytes long.  
  
  You can specify the key input format that you want to use to enter the Cisco ISE FIPS encryption key, so that it matches the configuration that is available on the WLC. The value that you specify must be the correct (full) length for the key. Shorter values are not permitted. |
| TACACS Authentication Settings       |                  |
## Device Security Settings

Specify the minimum length for the RADIUS shared secret. For new installation and upgraded deployment, by default, this value is 4 characters. For the RADIUS server, best practice is to have 22 characters.

### Fields

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared Secret</td>
<td>A string of text assigned to a network device when TACACS+ protocol is enabled. A user must enter the text before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.</td>
</tr>
<tr>
<td>Retired Shared Secret is Active</td>
<td>Displayed when the retirement period is active.</td>
</tr>
<tr>
<td>Retire</td>
<td>Retires an existing shared secret instead of ending it. When you click Retire, a message box is displayed. You can either click Yes or No.</td>
</tr>
<tr>
<td>Remaining Retired Period</td>
<td>(Available only if you select Yes in the above message box) Displays the default value specified in the following navigation path: Work Centers &gt; Device Administration &gt; Settings &gt; Connection Settings &gt; Default Shared Secret Retirement Period. You can change the default values. This allows a new shared secret to be entered and the old shared secret will remain active for the specified number of days.</td>
</tr>
<tr>
<td>End</td>
<td>(Available only if you select Yes in the above message box) Ends the retirement period and terminates the old shared secret.</td>
</tr>
</tbody>
</table>
| Enable Single Connect Mode    | Check to use a single TCP connection for all TACACS+ communication with the network device. Choose one of the following:  
  • Legacy Cisco Devices  
  • Or, TACACS+ Draft Compliance Single Connect Support. If you disable this option, ISE uses a new TCP connection for every TACACS+ request. |

### Device Security Settings

Specify the minimum length for the RADIUS shared secret. For new installation and upgraded deployment, by default, this value is 4 characters. For the RADIUS server, best practice is to have 22 characters.

**Note**

The length of the shared secret entered in the Network Devices page must be equal to or greater than the value configured in the Minimum RADIUS Shared Secret Length field in the Device Security Settings page.

**Related Topics**

Network Device Definition Settings, on page 988
Network Device Import Settings

The following table describes the fields on the Network Device Import Page, which you can use to import network device details into Cisco ISE. The navigation path for this page is: Administration > Network Resources > Network Devices.

**Table 118: Network Devices Import Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate a Template</td>
<td>Click this link to create a comma-separated value (.csv) template file. You must update the template with network devices information in the same format, and save it locally to import those network devices into any Cisco ISE deployment.</td>
</tr>
<tr>
<td>File</td>
<td>Click <strong>Browse</strong> to the location of the comma-separated value file that you might have created or previously exported from any Cisco ISE deployment. You can import network devices in another Cisco ISE deployment with new and updated network devices information using import.</td>
</tr>
<tr>
<td>Overwrite Existing Data with New Data</td>
<td>Check this check box if you want Cisco ISE to replace existing network devices with the devices in your import file. If you do not check this check box, new network device definitions that are available in the import file are added to the network device repository. Duplicate entries are ignored.</td>
</tr>
<tr>
<td>Stop Import on First Error</td>
<td>Check this check box if you want Cisco ISE to discontinue import when it encounters an error during import, but Cisco ISE imports network devices until that time of an error. If this check box is not checked and an error is encountered, the error is reported, and Cisco ISE continues to import devices.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Network Devices Definitions in Cisco ISE, on page 209
- Third-Party Network Device Support in Cisco ISE, on page 212
- Import Network Devices into Cisco ISE, on page 211

Network Device Groups

These pages enable you to configure and manage network device groups.
Network Device Group Settings

The following table describes the fields on the Network Device Groups Page, which you can use to create network device groups. The navigation path for this page is: Administration > Network Resources > Network Device Groups > Groups.

You can also create network device groups in the Work Centers > Device Administration > Network Device Groups > Groups page.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name for the root Network Device Group (NDG). For all subsequent child network device groups under the root NDG, enter the name of the new network device group. You can have a maximum of six nodes in the NDG hierarchy, including the root node. Each NDG name can have a maximum of 32 characters.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description for the root or the child Network Device Group.</td>
</tr>
<tr>
<td>Parent Group</td>
<td>You can select an already existing group as the parent group or add this new group as a root group.</td>
</tr>
</tbody>
</table>

Related Topics
- Network Device Groups, on page 219
- Network Device Attributes Used By Cisco ISE in Policy Evaluation, on page 220
- Create a Network Device Definition in Cisco ISE, on page 188

Network Device Group Import Settings

The following table describes the fields on the Network Device Group Import Page, which you can use to import network device groups into Cisco ISE. The navigation path for this page is: Administration > Network Resources > Network Device Groups > Groups.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate a Template</td>
<td>Click this link to create a comma-separated value (.csv) template file. You must update the template with network device groups information in the same format, and save it locally to import those network device groups into any Cisco ISE deployment.</td>
</tr>
</tbody>
</table>
Network Device Profiles Settings

The following table describes the fields on the Network Device Profiles page, which you can use to configure the default settings for a type of network device from a specific vendor, such as the device's support for protocols, redirect URLs, and CoA settings. You then use the profile to define specific network devices.

The navigation path for this page is: Administration > Network Resources > Network Device Profiles.

**Table 121: Network Device Profile Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name for the network device profile.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description for the network device profile.</td>
</tr>
</tbody>
</table>
### Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Icon</strong></td>
<td>Select the icon to use for the network device profile. This icon will default to the icon for the vendor that you select. The icon you select must be a 16 x 16 PNG file.</td>
</tr>
<tr>
<td><strong>Vendor</strong></td>
<td>Select the vendor of the network device profile. The vendors available for selection are Cisco, Aruba, HP, Motorola, Brocade, Alcatel, and Other.</td>
</tr>
<tr>
<td><strong>Supported Protocols</strong></td>
<td></td>
</tr>
<tr>
<td>RADIUS</td>
<td>Check this check box if this network device profile supports RADIUS.</td>
</tr>
<tr>
<td>TACACS+</td>
<td>Check this check box if this network device profile supports TACACS+.</td>
</tr>
<tr>
<td>TrustSec</td>
<td>Check this check box if this network device profile supports TrustSec.</td>
</tr>
<tr>
<td>RADIUS Dictionaries</td>
<td>Select one or more RADIUS dictionaries supported by this profile. Import any vendor-specific RADIUS dictionaries before you create the profile.</td>
</tr>
</tbody>
</table>

### Authentication/Authorization Template Settings

The following table describes the fields in the Authentication/Authorization section.
### Table 122: Authentication/Authorization Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow Type Conditions</td>
<td>Cisco ISE supports 802.1X, MAC authentication bypass (MAB), and browser-based Web authentication login for basic user authentication and access via both wired and wireless networks.</td>
</tr>
<tr>
<td></td>
<td>Check the check boxes for the authentication logins that this type of network device supports. It could be one or more of the following:</td>
</tr>
<tr>
<td></td>
<td>• Wired MAC authentication bypass (MAB)</td>
</tr>
<tr>
<td></td>
<td>• Wireless MAB</td>
</tr>
<tr>
<td></td>
<td>• Wired 802.1X</td>
</tr>
<tr>
<td></td>
<td>• Wireless 802.1X</td>
</tr>
<tr>
<td></td>
<td>• Wired Web Authentication</td>
</tr>
<tr>
<td></td>
<td>• Wireless Web Authentication</td>
</tr>
<tr>
<td></td>
<td>After you check the authentication logins that the network device profile supports, specify the conditions for the login.</td>
</tr>
<tr>
<td>Attribute Aliasing</td>
<td>Check the SSID check box to use the device’s Service Set Identifier (SSID) as the friendly name in policy rules. This allows you to create a consistent name to use in policy rules and it will work for multiple devices.</td>
</tr>
<tr>
<td>Host Lookup (MAB)</td>
<td></td>
</tr>
<tr>
<td>Process Host Lookup</td>
<td>Check this check box to define the protocols for host lookup used by the network device profile.</td>
</tr>
<tr>
<td></td>
<td>Network devices from different vendors perform MAB authentication differently. Depending on the device type, check the Check Password check, the Checking Calling-Station-Id equals MAC Address check box, or both, for the protocol you are using.</td>
</tr>
<tr>
<td>Via PAP/ASCII</td>
<td>Check this check box to configure Cisco ISE to detect a PAP request from the network device profile as a Host Lookup request.</td>
</tr>
</tbody>
</table>
Permissions Template Settings

You can define the VLAN and ACL permissions that will be used for this network device profile. After the profile is saved, Cisco ISE automatically generates authorization profiles for each configured permission. The following table describes the fields in the Permissions section.

Table 123: Permissions Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set VLAN</td>
<td>Check this check box to set the VLAN permissions for this network device profile. Choose of the following options:</td>
</tr>
<tr>
<td></td>
<td>• IETF 802.1X Attributes. This is a set of default RADIUS attributes defined by the Internet Engineering Task Force.</td>
</tr>
<tr>
<td></td>
<td>• Unique Attributes. You can specify multiple RADIUS attribute-value pairs.</td>
</tr>
<tr>
<td>Set ACL</td>
<td>Check this check box to select the RADIUS attribute to set for the ACL on the network device profile.</td>
</tr>
</tbody>
</table>

Change of Authorization (CoA) Template Settings

This template defines how the CoA is sent to this type of network device. The following table describes the fields in the Change of Authorization (CoA) section.

Table 124: Change of Authorization (CoA) Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>CoA by</td>
<td>Select whether to deliver the CoA packets to the network device profile by RADIUS, by SNMP or not at all.</td>
</tr>
<tr>
<td>CoA by RADIUS</td>
<td></td>
</tr>
<tr>
<td>Fields</td>
<td>Definition</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default CoA Port</td>
<td>The port to send the RADIUS CoA. By default, this is port 1700 for Cisco devices and port 3799 for devices from a non-Cisco vendor. You can override this on the Network Device page.</td>
</tr>
<tr>
<td>Timeout Interval</td>
<td>The number of seconds that Cisco ISE waits for a response after sending the CoA.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>The number of times Cisco ISE attempts to send the CoA after the first timeout.</td>
</tr>
<tr>
<td>Disconnect</td>
<td>Select how to send a disconnect request to these devices.</td>
</tr>
<tr>
<td></td>
<td>• RFC 5176. Check this check box for a standard session termination and leave the port ready for a new session, as defined per RFC 5176.</td>
</tr>
<tr>
<td></td>
<td>• Port Bounce. Check this check box to terminate the session and restart the port.</td>
</tr>
<tr>
<td></td>
<td>• Port Shutdown. Check this check box to terminate the session and shutdown the port.</td>
</tr>
<tr>
<td>Re-authenticate</td>
<td>Select how to send a reauthentication request to the network devices. This is currently supported only by Cisco devices.</td>
</tr>
<tr>
<td></td>
<td>• Basic. Check this check box for a standard session reauthentication.</td>
</tr>
<tr>
<td></td>
<td>• Rerun. Check this check box to run through the authentication method from the beginning.</td>
</tr>
<tr>
<td></td>
<td>• Last. Use the last successful authentication method for the session.</td>
</tr>
<tr>
<td>CoA Push</td>
<td>If the network devices do not support Cisco's TrustSec CoA feature, select this option to allow Cisco ISE to push a configuration change to the device.</td>
</tr>
<tr>
<td>CoA by SNMP</td>
<td></td>
</tr>
<tr>
<td>Timeout Interval</td>
<td>The number of seconds that Cisco ISE waits for a response after sending the CoA.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>The number of times that Cisco ISE attempts to send a CoA.</td>
</tr>
<tr>
<td>NAD Port Detection</td>
<td>Relevant RADIUS attribute is currently the only option.</td>
</tr>
</tbody>
</table>
### Redirect Template Settings

The network devices can redirect a client's HTTP requests if it's configured as part of the authorization profile. This template specifies whether this network device profile supports URL redirect. You will use the URL parameter names specific to the device type.

The following table describes the fields in the Redirect section.

**Table 125: Redirect Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select whether the network device profile supports a static or dynamic URL redirect. If your device supports neither, select Not Supported and set up a VLAN from Settings &gt; DHCP &amp; DNS Services.</td>
</tr>
<tr>
<td>Redirect URL Parameter Names</td>
<td></td>
</tr>
<tr>
<td>Client IP Address</td>
<td>Enter the parameter name that the network devices use for a client's IP address.</td>
</tr>
<tr>
<td>Client MAC Address</td>
<td>Enter the parameter name that the network devices use for a client's MAC address.</td>
</tr>
<tr>
<td>Originating URL</td>
<td>Enter the parameter name that the network devices use for the originating URL.</td>
</tr>
<tr>
<td>Session ID</td>
<td>Enter the parameter name that the network devices use for the session ID.</td>
</tr>
<tr>
<td>SSID</td>
<td>Enter the parameter name that the network devices use for the Service Set Identifier (SSID).</td>
</tr>
</tbody>
</table>
### Advanced Settings

You can use the Network Device Profile to generate a number of policy elements to make it easy to use a network device in policy rules. These elements include compound conditions, authorization profiles, and allowed protocols.

Click the **Generate Policy Elements** button to create these elements.

**Related Topics**
- [Network Device Profiles](#), on page 215
- [Third-Party Network Device Support in Cisco ISE](#), on page 212
- [Create a Network Device Profile](#), on page 217

### External RADIUS Server Settings

The following table describes the fields on the External RADIUS Server page, which you can use to configure a RADIUS server. For Cisco ISE to act as a RADIUS server, you must configure it in this page. The navigation path for this page is: **Administration > Network Resources > External RADIUS Servers**.

**Table 126: External RADIUS Server Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the external RADIUS server.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the external RADIUS server.</td>
</tr>
<tr>
<td>Host IP</td>
<td>Enter the IP address of the external RADIUS server.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared secret between Cisco ISE and the external RADIUS server that is used for authenticating the external RADIUS server. A shared secret is an expected string of text that a user must provide to enable the network device to authenticate a username and password. The connection is rejected until the user supplies the shared secret. The shared secret can be up to 128 characters in length.</td>
</tr>
<tr>
<td>Enable KeyWrap</td>
<td>Enable this option to increase the RADIUS protocol security via an AES KeyWrap algorithm, to help enable FIPS 140-2 compliance in Cisco ISE.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Key Encryption Key</td>
<td>(Only if you check the Enable Key Wrap check box) Enter a key to be used for session encryption (secrecy).</td>
</tr>
<tr>
<td>Message Authenticator Code Key</td>
<td>(Only if you check the Enable Key Wrap check box) Enter a key to be used for keyed HMAC calculation over RADIUS messages.</td>
</tr>
<tr>
<td>Key Input Format</td>
<td>Specify the format you want to use to enter the Cisco ISE encryption key, so that it matches the configuration that is available on the WLAN controller. (The value you specify must be the correct [full] length for the key as defined below—shorter values are not permitted.)</td>
</tr>
<tr>
<td></td>
<td>• ASCII—The Key Encryption Key must be 16 characters (bytes) long, and the Message Authenticator Code Key must be 20 characters (bytes) long.</td>
</tr>
<tr>
<td></td>
<td>• Hexadecimal—The Key Encryption Key must be 32 bytes long, and the Message Authenticator Code Key must be 40 bytes long.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>Enter the RADIUS authentication port number. The valid range is from 1 to 65535. The default is 1812.</td>
</tr>
<tr>
<td>Accounting Port</td>
<td>Enter the RADIUS accounting port number. The valid range is from 1 to 65535. The default is 1813.</td>
</tr>
<tr>
<td>Server Timeout</td>
<td>Enter the number of seconds that the Cisco ISE waits for a response from the external RADIUS server. The default is 5 seconds. Valid values are from 5 to 120.</td>
</tr>
<tr>
<td>Connection Attempts</td>
<td>Enter the number of times that the Cisco ISE attempts to connect to the external RADIUS server. The default is 3 attempts. Valid values are from 1 to 9.</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Cisco ISE Acting as a RADIUS Proxy Server](on page 588)
- [Configure External RADIUS Servers](on page 589)

**RADIUS Server Sequences**

The following table describes the fields on the RADIUS Server Sequences page, which you can use to create a RADIUS server sequence. The navigation path for this page is: Administration > Network Resources > RADIUS Server Sequences > Add.
Table 127: RADIUS Server Sequences

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the RADIUS server sequence.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter an optional description.</td>
</tr>
<tr>
<td>Host IP</td>
<td>Enter the IP address of the external RADIUS server.</td>
</tr>
<tr>
<td>User Selected Service Type</td>
<td>Choose the external RADIUS servers that you want to use as policy servers from the Available list box and move them to the Selected list box.</td>
</tr>
<tr>
<td>Remote Accounting</td>
<td>Check this check box to enable accounting in the remote policy server.</td>
</tr>
<tr>
<td>Local Accounting</td>
<td>Check this check box to enable accounting in Cisco ISE.</td>
</tr>
</tbody>
</table>

**Advanced Attribute Settings**

| Strip Start of Subject Name up to the First Occurrence of the Separator | Check this check box to strip the username from the prefix. For example, if the subject name is acme\userA and the separator is \, the username becomes userA. |
| Strip End of Subject Name from the Last Occurrence of the Separator   | Check this check box to strip the username from the suffix. For example, if the subject name is userA@abc.com and the separator is @, the username becomes userA. |

- You must enable the strip options to extract the username from NetBIOS or User Principle Name (UPN) format usernames (user@domain.com or /domain/user), because only usernames are passed to the RADIUS server for authenticating the user.

- If you activate both the \ and @ stripping functions, and you are using Cisco AnyConnect, Cisco ISE does not accurately trim the first \ from the string. However, each stripping function that is used individually, however, works as it is designed with Cisco AnyConnect.
Usage Guidelines

Fields

Modify Attributes in the Request to the External RADIUS Server

Check this check box to allow Cisco ISE to manipulate attributes that come from or go to the authenticated RADIUS server.

The attribute manipulation operations include these:

- **Add**—Add additional attributes to the overall RADIUS request/response.
- **Update**—Change the attribute value (fixed or static) or substitute an attribute by another attribute value (dynamic).
- **Remove**—Remove an attribute or an attribute-value pair.
- **RemoveAny**—Remove any occurrences of the attribute.

Continue to Authorization Policy

Check this check box to divert the proxy flow to run the authorization policy for further decision making, based on identity store group and attribute retrieval. If you enable this option, attributes from the response of the external RADIUS server will be applicable for the authentication policy selection. Attributes that are already in the context will be updated with the appropriate value from the AAA server accept response attribute.

Modify Attributes before send an Access-Accept

Check this check box to modify the attribute just before sending a response back to the device.

Related Topics

- Cisco ISE Acting as a RADIUS Proxy Server, on page 588
- Define RADIUS Server Sequences, on page 589

NAC Manager Settings

The following table describes the fields on the New NAC Managers page, which you can use to add a NAC Manager. The navigation path for this page is: Administration > Network Resources > NAC Managers.

Table 128: NAC Manager Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the Cisco Access Manager (CAM).</td>
</tr>
<tr>
<td>Status</td>
<td>Click the Status check box to enable REST API communication from the Cisco ISE profiler that authenticates connectivity to the CAM.</td>
</tr>
</tbody>
</table>
## Device Portal Management

### Configure Device Portal Settings

#### Global Settings for Device Portals

Choose **Work Centers > BYOD > Settings > Employee Registered Devices** or **Administration > Device Portal Management > Settings**.

You can configure the following general settings for the BYOD and My Devices portals:

- **Employee Registered Devices**—Enter the maximum number of devices that an employee can register in **Restrict employees to**. By default, this value is set to 5 devices.

- **Retry URL**—Enter a URL that can be used to redirect the device back to Cisco ISE in **Retry URL for onboarding**.

Once you configure these general settings, they apply to all BYOD and My Devices portals that you set up for your company.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter the description of the CAM.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the CAM. Once you have created and saved a CAM in Cisco ISE, the IP address of the CAM cannot be edited. You cannot use 0.0.0.0 and 255.255.255.255, as they are excluded when validating the IP addresses of the CAMs in Cisco ISE, and so, they are not valid IP addresses that you can use in the IP Address field for the CAM. <strong>Note</strong> You can use the virtual service IP address that a pair of CAMs share in a high-availability configuration. This allows a failover support of CAMs in a high-availability configuration.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username of the CAM administrator that allows you to log on to the user interface of the CAM.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password of the CAM administrator that allows you to log on to the user interface of the CAM.</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Cisco ISE Integration with Cisco NAC Appliance](#), on page 688
- [Add Cisco Clean Access Managers](#), on page 690
Portal Identification Settings for Device Portals

The navigation path for these settings is Administration > Device Portal Managment > Blacklist Portal, Client Provisioning Portals, BYOD Portals, MDM Portals, or My Device Portals > Create, Edit or Duplicate > Portals Settings and Customization.

- **Portal Name**—Enter a unique portal name to access this portal. Do not use this portal name for any other Sponsor and Guest portals and non-guest portals, such as Blacklist, Bring Your Own Device (BYOD), Client Provisioning, Mobile Device Management (MDM), or My Devices portals.

  This name appears in the authorization profile portal selection for redirection choices, and is used in the list of portals for easy identification among other portals.

- **Description**—Optional.

- **Portal test URL**—A system-generated URL displays as a link after you click Save. Use it to test the portal.

  Click the link to open a new browser tab that displays the URL for this portal. In order for this to work, Policy Services Node (PSN) with Policy Services must be turned on. If Policy Services are not turned on, the PSN only displays the Admin portal.

  **Note**

  The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. For example, a redirect to an external URL will not work.

- **Language File**—Each portal type supports 15 languages by default, which are available as individual properties files bundled together in a single zipped language file. Export or import the zipped language file to use with the portal. The zipped language file contains all the individual language files that you can use to display text for the portal.

  The language file contains the mapping to the particular browser locale setting (for example, for French: fr, fr-fr, fr-ca) along with all of the string settings for the entire portal in that language. A single language file contains all the supported languages, so that it can easily be used for translation and localization purposes.

  If you change the browser locale setting for one language, the change is applied to all the other end-user web portals. For example, if you change the French.properties browser locale from fr,fr-fr,fr-ca to fr,fr-fr in the Hotspot Guest portal, the change is applied to the My Devices portal also.

  An alert icon displays when you customize any of the portal page text on the Portal Page Customizations tab. The alert message reminds you to update any changes made to one language while customizing the portal into all the supported languages properties files. You can manually dismiss the alert icon using the drop-down list option; or it is automatically dismissed after you import the updated zipped language file.
Portal Settings for the Blacklist Portal

The navigation path for these settings is Administration > Device Portal Management > Blacklist Portal > Edit > Portal Behavior and Flow Settings > Portal Settings

Use these settings to specify values or define behavior that applies to the overall portal; not just to specific portal pages that display to the user (guests, sponsors, or employees as applicable).

- **HTTP port**—Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you modify this page. If you modify this page, update the port setting to comply with this restriction.

If you assign Ports used by a non-guest (such as My Devices) portal to a guest portal, an error message displays.

For posture assessments and remediation only, the Client Provisioning portal also uses Ports 8905 and 8909. Otherwise, it uses the same Ports assigned to the Guest portal.

Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

- **Valid combinations** include, using the Sponsor portal as an example:
  - Sponsor portal: Port 8443, Interface 0, Certificate tag A and My Devices portal: Port 8443, Interface 0, Certificate group A.
  - Sponsor portal: Port 8443, Interface 0, Certificate group A and My Devices portal: Port 8445, Interface 0, Certificate group B.
  - Sponsor portal: Port 8444, Interface 1, Certificate group A and Blacklist portal: Port 8444, Interface 0, Certificate group B.

- **Invalid combinations** include:
  - Sponsor portal: Port 8443, Interface 0, Certificate group A and My Devices portal: 8443, Interface 0, Certificate group B.
  - Sponsor portal: Port 8444, Interface 0, Certificate tag A and Blacklist portal: Port 8444, Interface 0, Certificate group A.

- **Allowed interfaces** — Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed Port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets.

These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.
• The Ethernet interfaces must use IP addresses on different subnets.

• The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.

• The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP.

• Configure `ip host x.x.x.x yyy.domain.com` in ISE CLI to map secondary interface IP to FQDN, which is used to match Certificate Subject Name / Alternate Subject Name.

• If only the bonded NIC is selected - When the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN logs an error and exits. The PSN will NOT try to start the portal on the physical interface.

• **NIC teaming** or bonding is an O/S configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based on the portal settings configuration:
  - If both physical NICs and the corresponding bonded NIC are configured - When the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

• **Certificate group tag** — Pick a certificate group tag that specifies the certificate to use for the portal’s HTTPS traffic.

• **Display Language**
  - **Use browser locale** — Use the language specified in the client browser's locale setting as the display language of the portal. If browser locale's language is not supported by ISE, then the Fallback Language is used as the language portal.

  - **Fallback language** — Choose the language to use when language cannot be obtained from the browser locale, or if the browser locale language is not supported by ISE.

  - **Always use** — Choose the display language to use for the portal. This setting overrides the User browser locale option.

SSIDs available to sponsors — Enter the names or the SSIDs (Session Service Identifiers) of the networks that a sponsor can notify guests as the correct networks to connect to for their visit.

**Related Topics**

- Edit the Blacklist Portal, on page 507
- Blacklist Portal, on page 497
- HTML Support for the Blacklist Portal Language File, on page 1068

**Portal Settings for BYOD and MDM Portals**

The navigation path for these settings is Administration > Device Portal Management > BYOD Portals or MDM Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Portal Settings.
Configure these settings to define portal page operations.

- **HTTPS port**—Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you modify this page. If you modify this page, update the port setting to comply with this restriction.

If you assign Ports used by a non-guest (such as My Devices) portal to a guest portal, an error message displays.

For posture assessments and remediation only, the Client Provisioning portal also uses Ports 8905 and 8909. Otherwise, it uses the same Ports assigned to the Guest portal.

Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

- **Valid combinations** include, using the Sponsor portal as an example:
  - Sponsor portal: Port 8443, Interface 0, Certificate tag A and My Devices portal: Port 8443, Interface 0, Certificate group A.
  - Sponsor portal: Port 8443, Interface 0, Certificate group A and My Devices portal: Port 8445, Interface 0, Certificate group B.
  - Sponsor portal: Port 8444, Interface 1, Certificate group A and Blacklist portal: Port 8444, Interface 0, Certificate group B.

- **Invalid combinations** include:
  - Sponsor portal: Port 8443, Interface 0, Certificate group A and My Devices portal: 8443, Interface 0, Certificate group B.
  - Sponsor portal: Port 8444, Interface 0, Certificate tag A and Blacklist portal: Port 8444, Interface 0, Certificate group A.

- **Allowed interfaces** — Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed Port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets. These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.

  - The Ethernet interfaces must use IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  - The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP.
  - Configure `ip host x.x.x.x yyyy.domain.com` in ISE CLI to map secondary interface IP to FQDN, which is used to match Certificate Subject Name / Alternate Subject Name.
  - If only the bonded NIC is selected - When the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup...
on that PSN, then the PSN logs an error and exits. The PSN will NOT try to start the portal on the physical interface.

• **NIC teaming** or bonding is an O/S configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based on the portal settings configuration:
  • If both physical NICs and the corresponding bonded NIC are configured - When the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

• **Certificate group tag**—Pick a certificate group tag that specifies the certificate to use for the portal’s HTTPS traffic.

• **Endpoint identity group**—Choose an endpoint identity group to track guest devices. Cisco ISE provides the *GuestEndpoints* endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

Choose an endpoint identity group to track employee devices. Cisco ISE provides the *RegisteredDevices* endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

• **Display Language**
  • **Use browser locale**—Use the language specified in the client browser's locale setting as the display language of the portal. If browser locale's language is not supported by ISE, then the Fallback Language is used as the language portal.

  • **Fallback language**—Choose the language to use when language cannot be obtained from the browser locale, or if the browser locale language is not supported by ISE.

  • **Always use**—Choose the display language to use for the portal. This setting overrides the User browser locale option.

SSIDs available to sponsors—Enter the names or the SSIDs (Session Service Identifiers) of the networks that a sponsor can notify guests as the correct networks to connect to for their visit.

**Related Topics**
- Bring Your Own Device Portal, on page 498
- Create a BYOD Portal, on page 509
- Mobile Device Management Portal, on page 498
- Create an MDM Portal, on page 512
- HTML Support for Bring Your Own Device Portals Language Files, on page 1069
- HTML Support for Mobile Device Management Portals Language Files, on page 1075

**BYOD Settings for BYOD Portals**

The navigation path for these settings is Administration > Device Portal Management > BYOD Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > BYOD Settings.
Use these settings to enable Bring Your Own Device (BYOD) functionality for employees who want to use their personal devices to access your corporate network.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include an AUP (on page/as link)</td>
<td>Display your company’s network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.</td>
</tr>
<tr>
<td>Require acceptance</td>
<td>Require users to accept an AUP before their account is fully enabled. The Login button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not obtain network access.</td>
</tr>
<tr>
<td>Require scrolling to end of AUP</td>
<td>This option displays only if Include an AUP on page is enabled. Ensure that the user has read the AUP completely. The Accept button activates only after the user has scrolled to the end of the AUP.</td>
</tr>
<tr>
<td>Display Device ID field during registration</td>
<td>Display the device ID to the user during the registration process, even though the device ID is pre-configured and cannot be changed while using the BYOD portal.</td>
</tr>
<tr>
<td>Originating URL</td>
<td>After successfully authenticating to the network, redirect the user’s browser to the original website that the user is trying to access, if available. If not available, the Authentication Success page displays. Make sure that the redirect URL is allowed to work on port 8443 of the PSN by the access-control list on the NAD and by authorization profiles configured in ISE for that NAD. For Windows, MAC and Android devices, control is given to the Self-Provisioning Wizard app, which does provisioning. Therefore, these devices are not redirected to the originating URL. However, iOS (dot1X) and unsupported devices (that are allowed network access) are redirected to this URL.</td>
</tr>
<tr>
<td>Success page</td>
<td>Display a page indicating that the device registration was successful.</td>
</tr>
<tr>
<td>URL</td>
<td>After successfully authenticating to the network, redirect the user's browser to the specified URL, such as your company’s website.</td>
</tr>
</tbody>
</table>

If you redirect a Guest to an external URL after authentication, there may be a delay while the URL address is resolved and the session is redirected.
Portal Settings for Certificate Provisioning Portal

The navigation path for these settings is Administration > Device Portal Management > Certificate Provisioning Portal > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Portal Settings.

• **HTTPS port**—Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you modify this page. If you modify this page, update the port setting to comply with this restriction.

  If you assign Ports used by a non-guest (such as My Devices) portal to a guest portal, an error message displays.

For posture assessments and remediation only, the Client Provisioning portal also uses Ports 8905 and 8909. Otherwise, it uses the same Ports assigned to the Guest portal.

Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

• Valid combinations include, using the Sponsor portal as an example:
  * Sponsor portal: Port **8443**, Interface 0, Certificate tag A and My Devices portal: Port **8443**, Interface 0, Certificate tag A.
  * Sponsor portal: Port **8443**, Interface 0, Certificate group A and My Devices portal: Port **8445**, Interface 0, Certificate group B.
  * Sponsor portal: Port **8444**, Interface 1, Certificate group A and Blacklist portal: Port **8444**, Interface 0, Certificate group B.

• Invalid combinations include:
  * Sponsor portal: Port **8443**, Interface 0, Certificate group A and My Devices portal: **8443**, Interface 0, Certificate group B.
  * Sponsor portal: Port **8444**, Interface 0, Certificate tag A and Blacklist portal: Port **8444**, Interface 0, Certificate group A.

• **Allowed interfaces** — Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed Port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets.

  These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.

  * The Ethernet interfaces must use IP addresses on different subnets.
• The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.

• The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP.

• Configure `ip host x.x.x.x yyyy.domain.com` in ISE CLI to map secondary interface IP to FQDN, which is used to match Certificate Subject Name / Alternate Subject Name.

• If only the bonded NIC is selected - When the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN logs an error and exits. The PSN will NOT try to start the portal on the physical interface.

• NIC teaming or bonding is an O/S configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based on the portal settings configuration:
  - If both physical NICs and the corresponding bonded NIC are configured - When the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

• Certificate group tag—Pick a certificate group tag that specifies the certificate to use for the portal’s HTTPS traffic.

• Authentication Method—Choose which identity source sequence (ISS) or Identity Provider (IdP) to use for user authentication. The ISS is a list of Identity Stores that are searched in sequence to verify user credentials. Some examples include: Internal Guest Users, Internal Users, Active Directory, LDAP Directory.

Cisco ISE includes a default sponsor Identity Source Sequence for sponsor portals, Sponsor_Portal_Sequence.

To configure IdP, choose Administration > Identity Management > External Identity Sources > SAML Id Providers.

To configure an Identity Source Sequence, choose Administration > Identity Management > Identity Source Sequences.

• Configure authorized groups—Choose the user identity groups to which you want to grant permission to generate certificates and move them to the Chosen box.

• Fully Qualified Domain Name (FQDN)—Enter at least one unique FQDN and/or hostname for your Sponsor or MyDevices portal. For example, you can enter `sponsorportal.yourcompany.com`, so that when the user enters either of those into a browser, the sponsor portal displays. Separate names with commas, but do not include spaces between entries.

If you change the default FQDN, then also do the following:

• Update your DNS so that the FQDN of the new URL resolves to a valid Policy Services Node (PSN) IP address. Optionally, this address could point to a load balancer virtual IP address that serves a pool of PSNs.
To avoid certificate warning messages due to name mismatches, include the FQDN of the customized URL, or a wildcard, in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE PSN.

- **Idle timeout**—Enter the time in minutes that you want Cisco ISE to wait before it logs out the user if there is no activity in the portal. The valid range is from 1 to 30 minutes.

### Login Page Settings

- **Maximum failed login attempts before rate limiting**—Specify the number of failed login attempts from a single browser session before Cisco ISE starts to throttle that account. This does not cause an account lockout. The throttled rate is configured in **Time between login attempts when rate limiting**.

- **Include an AUP**—Add a acceptable use policy page to the flow. You can add the AUP to the page, or link to another page. Adding this changes the picture of the flow on the right.
  - **require acceptance**—Force the user to agree to the AUP before continuing the flow.

### Acceptable Use Policy (AUP) Page Settings

- **Include an AUP page**—Display your company’s network-usage terms and conditions on a separate page to the user.

- **Use different AUP for employees**—Display a different AUP and network-usage terms and conditions for employees only. If you choose this option, you cannot also choose **Skip AUP for employees**.

- **Skip AUP for employees**—Employees are not required to accept an AUP before accessing the network. If you choose this option, you cannot also choose **Use different AUP for employees**.

- **Require acceptance**—Require users to accept an AUP before their account is fully enabled. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not obtain network access.

- **Require scrolling to end of AUP**—This option displays only if **Include an AUP on page** is enabled. Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP. Configure when the AUP appears to the user.
  - **On first login only**—Display an AUP the first time the user logs into the network or portal.
  - **On every login**—Display an AUP every time the user logs into the network or portal.
  - **Every __ days (starting at first login)**—Display an AUP periodically after the user first logs into the network or portal.

### Related Topics

- [Certificate Provisioning Portal](#), on page 497
- [Create a Certificate Provisioning Portal](#), on page 510
- [HTML Support for Certificate Provisioning Portal Language Files](#), on page 1070
Portal Settings for Client Provisioning Portals

The navigation path for these settings is Administration > Device Portal Management > Client Provisioning Portals > Create, Edit, Duplicate, or Delete > Portal Behavior and Flow Settings.

Portal Settings

• **HTTPS Port**—Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you make any change to this page. If you make any change to this page, you must update the port setting to comply with this restriction.

• **Allowed Interfaces**—Select the PSN interfaces which can run a portal. Only a PSN with an available allowed interface on a PSN can create a portal. You can configure any combination of physical and bonded interfaces. This is a PSN-wide configuration; all portals can only run on these interfaces, this interface configuration is pushed to all the PSNs.
  - You must configure the Ethernet interfaces using IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  - The portal certificate Subject Name/Alternate Subject Name must resolve to the interface IP.
  - Configure ip host x.x.x.x yyy.domain.com in ISE CLI to map secondary interface IP to FQDN, which will be used to match Certificate Subject Name/Alternate Subject Name.
  - If only the bonded NIC is selected - When the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond set up upon that PSN, then the PSN logs an error and exits. It will NOT attempt to start the portal on the physical interface.

• **NIC Teaming** or bonding is an O/S configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based on the portal settings configuration:
  - If both physical NICs and the corresponding bonded NIC are configured - When the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

• **Certificate Group Tag**—Select the group tag of the certificate group to use for the portal’s HTTPS traffic.

• **Authentication Method**—Choose which identity source sequence (ISS) or Identity Provider (IdP) to use for user authentication. The ISS is a list of Identity Stores that are searched in sequence to verify user credentials. Some examples include: Internal Guest Users, Internal Users, Active Directory, and LDAP.
  Cisco ISE includes a default client provisioning Identity Source Sequence for Client Provisioning Portals, Certificate_Request_Sequence.
• **Fully Qualified Domain Name (FQDN)**—Enter at least one unique FQDN and/or hostname for your Client Provisioning portal. For example, you can enter provisionportal.yourcompany.com, so that when the user enters either of those into a browser, they will reach the Client Provisioning Portal.

• Update DNS to ensure that the FQDN of the new URL resolves to a valid Policy Services Node (PSN) IP address. Optionally, this address could point to a load balancer virtual IP address that serves a pool of PSNs.

• To avoid certificate warning messages due to name mismatches, include the FQDN of the customized URL, or a wildcard, in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE PSN.

---

**Note**

For Client Provisioning without URL redirection, the portal name that is entered in the Fully Qualified Domain Name (FQDN) field must be configured in the DNS configuration. This URL must be communicated to the users to enable Client Provisioning without URL redirection.

---

• **Idle Timeout**—Enter the time in minutes that you want Cisco ISE to wait before it logs out the user if there is no activity in the portal. The valid range is from 1 to 30 minutes.

---

**Note**

In the Client Provisioning Portal, you can define the port number and the certificate so that the host allows you to download the same certificate for Client Provisioning and Posture. If the portal certificate is signed by the officials certificate authority, you will not receive any security warning. If the certificate is self-signed, you will receive one security warning for both the portals and Cisco AnyConnect Posture component.

---

**Login Page Settings**

• Enable Login—Select this check box to enable the login step in the Client Provisioning Portal

• Maximum failed login attempts before rate limiting—Specify the number of failed login attempts from a single browser session before Cisco ISE starts to artificially slow down the rate at which login attempts can be made, preventing additional login attempts. The time between attempts after this number of failed logins is reached is specified in Time between login attempts when rate limiting.

• Time between login attempts when rate limiting—Set the length of time in minutes that a user must wait before attempting to log in again, after failing to log in the number of times defined in Maximum failed login attempts before rate limiting.

• Include an AUP (on page/as link)—Display your company’s network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.

• Require acceptance—Require users to accept an AUP before they can access the portal. The Login button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not be able to access the portal.

• Require scrolling to end of AUP—This option displays only if Include an AUP on page is enabled. Ensure that the user has read the AUP completely. The Accept button activates only after the user has scrolled to the end of the AUP.
**Acceptable Use Policy (AUP) Page Settings**

- Include an AUP—Display your company’s network-usage terms and conditions on a separate page to the user.
- Require scrolling to end of AUP—Ensure that the user has read the AUP completely. The Accept button activates only after the user has scrolled to the end of the AUP.
- On first login only—Display an AUP when the user logs into the network or portal for the first time only.
- On every login—Display an AUP each time the user logs into the network or portal.
- Every ______ days (starting at first login)—Display an AUP periodically after the user first logs into the network or portal.

**Post-Login Banner Page Settings**

Include a Post-Login Banner page—Display additional information after the users successfully log in and before they are granted network access.

**Change Password Settings**

Allow internal users to change their own passwords—Allow employees to change their passwords after they log in to the Client Provisioning Portal. This only applies to employees whose accounts are stored in the Cisco ISE database and not to those stored in external databases, such as Active Directory or LDAP.

**Related Topics**

- [Client Provisioning Portal](#), on page 498
- [Create a Client Provisioning Portal](#), on page 511
- [HTML Support for Client Provisioning Portals Language Files](#), on page 1071

**Employee Mobile Device Management Settings for MDM Portals**

The navigation path for these settings is **Administration** > **Device Portal Management** > **MDM Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Employee Mobile Device Management Settings**.

Use these settings to enable Mobile Device Management (MDM) functionality for employees using the MDM portals and define their AUP experience.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include an AUP (on page/as link)</td>
<td>Display your company’s network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.</td>
</tr>
<tr>
<td>Require acceptance</td>
<td>Require users to accept an AUP before their account is fully enabled. The Login button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not obtain network access.</td>
</tr>
<tr>
<td>Field</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Require scrolling to end of AUP</td>
<td>This option displays only if Include an AUP on page is enabled. Ensure that the user has read the AUP completely. The Accept button activates only after the user has scrolled to the end of the AUP.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Mobile Device Management Portal, on page 498
- Create an MDM Portal, on page 512
- Mobile Device Manager Interoperability with Cisco ISE, on page 6

**Portal Settings for My Devices Portals**

The navigation path for these settings is **Administration > Device Portal Management > My Devices Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Portal Settings**.

- **HTTPS port** — Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you modify this page. If you modify this page, update the port setting to comply with this restriction.

  If you assign Ports used by a non-guest (such as My Devices) portal to a guest portal, an error message displays.

  For posture assessments and remediation only, the Client Provisioning portal also uses Ports 8905 and 8909. Otherwise, it uses the same Ports assigned to the Guest portal.

  Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

  - **Valid combinations include**, using the Sponsor portal as an example:
    - Sponsor portal: Port 8443, Interface 0, Certificate tag A and My Devices portal: Port 8443, Interface 0, Certificate group A.
    - Sponsor portal: Port 8443, Interface 0, Certificate group A and My Devices portal: Port 8445, Interface 0, Certificate group B.
    - Sponsor portal: Port 8444, Interface 1, Certificate group A and Blacklist portal: Port 8444, Interface 0, Certificate group B.

  - **Invalid combinations include**:
    - Sponsor portal: Port 8443, Interface 0, Certificate group A and My Devices portal: 8443, Interface 0, Certificate group B.
    - Sponsor portal: Port 8444, Interface 0, Certificate tag A and Blacklist portal: Port 8444, Interface 0, Certificate group A.

  - **Allowed interfaces** — Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed Port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets.
These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.

• The Ethernet interfaces must use IP addresses on different subnets.

• The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.

• The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP.

• Configure `ip host x.x.x.x yyyy.domain.com` in ISE CLI to map secondary interface IP to FQDN, which is used to match Certificate Subject Name / Alternate Subject Name.

• If only the bonded NIC is selected - When the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN logs an error and exits. The PSN will NOT try to start the portal on the physical interface.

• NIC teaming or bonding is an O/S configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based on the portal settings configuration:

  • If both physical NICs and the corresponding bonded NIC are configured - When the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

• Certificate group tag—Pick a certificate group tag that specifies the certificate to use for the portal’s HTTPS traffic.

• Fully Qualified Domain Name (FQDN)—Enter at least one unique FQDN and/or hostname for your Sponsor or MyDevices portal. For example, you can enter `sponsorportal.yourcompany.com,sponsor`, so that when the user enters either of those into a browser, the sponsor portal displays. Separate names with commas, but do not include spaces between entries.

  If you change the default FQDN, then also do the following:

  • Update your DNS so that the FQDN of the new URL resolves to a valid Policy Services Node (PSN) IP address. Optionally, this address could point to a load balancer virtual IP address that serves a pool of PSNs.

  • To avoid certificate warning messages due to name mismatches, include the FQDN of the customized URL, or a wildcard, in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE PSN.

• Authentication Method—Choose which identity source sequence (ISS) or Identity Provider (IdP) to use for user authentication. The ISS is a list of Identity Stores that are searched in sequence to verify user credentials. Some examples include: Internal Guest Users, Internal Users, Active Directory, LDAP Directory.

  Cisco ISE includes a default sponsor Identity Source Sequence for sponsor portals, Sponsor_Portal_Sequence.
To configure IdP, choose Administration > Identity Management > External Identity Sources > SAML Id Providers.

To configure an Identity Source Sequence, choose Administration > Identity Management > Identity Source Sequences.

- **Endpoint identity group**—Choose an endpoint identity group to track guest devices. Cisco ISE provides the GuestEndpoints endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

Choose an endpoint identity group to track employee devices. Cisco ISE provides the RegisteredDevices endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

- **Purge endpoints in this identity group when they reach ___ days**—Change the number of days since the registration of a user's device before it is purged from the Cisco ISE database. Purging is done on a daily basis and the purge activity is synchronized with the overall purge timing. The change is applied globally for this endpoint identity group.

If changes are made to the Endpoint Purge Policy based on other policy conditions, this setting is no longer available for use.

- **Idle timeout**—Enter the time in minutes that you want Cisco ISE to wait before it logs out the user if there is no activity in the portal. The valid range is from 1 to 30 minutes.

- **Display Language**
  - **Use browser locale**—Use the language specified in the client browser's locale setting as the display language of the portal. If browser locale's language is not supported by ISE, then the Fallback Language is used as the language portal.
  
  - **Fallback language**—Choose the language to use when language cannot be obtained from the browser locale, or if the browser locale language is not supported by ISE.
  
  - **Always use**—Choose the display language to use for the portal. This setting overrides the User browser locale option.

SSIDs available to sponsors—Enter the names or the SSIDs (Session Service Identifiers) of the networks that a sponsor can notify guests as the correct networks to connect to for their visit.

**Related Topics**
- My Devices Portal, on page 499
- Create a My Devices Portal, on page 514

**Login Page Settings for My Devices Portals**

- **Maximum failed login attempts before rate limiting**—Specify the number of failed login attempts from a single browser session before Cisco ISE starts to throttle that account. This does not cause an account lockout. The throttled rate is configured in **Time between login attempts when rate limiting**.

- **Maximum failed login attempts before rate limiting**—Specify the number of failed login attempts from a single browser session before Cisco ISE starts to throttle that account. This does not cause an account lockout. The throttled rate is configured in **Time between login attempts when rate limiting**.
• **Include an AUP**—Add a acceptable use policy page to the flow. You can add the AUP to the page, or link to another page. Adding this changes the picture of the flow on the right.

• **require acceptance**—Force the user to agree to the AUP before continuing the flow.

**Related Topics**

- **My Devices Portal**, on page 499
- **Create a My Devices Portal**, on page 514
- **Monitor My Devices Portals and Endpoints Activity**, on page 517

### Acceptable Use Policy Page Settings for My Devices Portals

The navigation path for this page is **Work Centers > Administration > Device Portal Management > My Devices Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Acceptable Use Policy (AUP) Page Settings**.

Use these settings to define the AUP experience for the users (guests, sponsors or employees as applicable).

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include an AUP page</td>
<td>Display your company’s network-usage terms and conditions on a separate page to the user.</td>
</tr>
<tr>
<td>Require scrolling to end of AUP</td>
<td>Ensure that the user has read the AUP completely. The <strong>Accept</strong> button activates only after the user has scrolled to the end of the AUP.</td>
</tr>
<tr>
<td>On first login only</td>
<td>Display an AUP when the user logs into the network or portal for the first time only.</td>
</tr>
<tr>
<td>On every login</td>
<td>Display an AUP each time the user logs into the network or portal.</td>
</tr>
<tr>
<td>Every __ days (starting at first login)</td>
<td>Display an AUP periodically after the user first logs into the network or portal.</td>
</tr>
</tbody>
</table>

**Related Topics**

- **My Devices Portal**, on page 499
- **Create a My Devices Portal**, on page 514

### Post-Login Banner Page Settings for My Devices Portals

The navigation path for this page is **Administration > Device Portal Management > My Devices Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Post-Login Banner Page Settings**.

Use this setting to notify users (guests, sponsors or employees as applicable) of additional information after they log in successfully.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include a Post-Login Banner page</td>
<td>Display additional information after the users successfully log in and before they are granted network access.</td>
</tr>
</tbody>
</table>
Employee Change Password Settings for My Devices Portals

The navigation path for this page is Administration > Device Portal Management > My Devices Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Employee Change Password Settings. Use these settings to define the password requirements for employees using the My Devices portal.

To set the employee password policy, choose Administration > Identity Management > Settings > Username Password Policy.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow internal users to change password</td>
<td>Allow employees to change their passwords after they log into the My Devices portal. This only applies to employees whose accounts are stored in the Cisco ISE database and not to those stored in external databases, such as Active Directory or LDAP.</td>
</tr>
</tbody>
</table>

Manage Device Settings for My Devices Portal

The navigation path for these settings is Administration > Device Portal Management > My Devices Portals > Create, Edit or Duplicate > Portal Page Customization > Manage Devices.

Under Page Customizations, you can customize the messages, titles, content, instructions, and field and button labels that appear on the Manage Accounts tab of the My Devices portal.

Under Settings, you can specify the actions that employees using this My Devices portal can perform on their registered personal devices.

Table 129: Manage Device Settings for My Devices Portals

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lost</td>
<td>For all devices. Enable employees to indicate that their device is lost. This action updates the device status in the My Devices portal to Lost and adds the device to the Blacklist endpoint identity group.</td>
</tr>
<tr>
<td>Field</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Reinstate</td>
<td>For all devices. This action reinstates a blacklisted, lost or stolen device and resets it status to its last known value. This action resets the status of a stolen device to Not Registered, since it has to undergo additional provisioning before it can connect to the network. If you want to prevent employees reinstating devices that you have blacklisted, do not enable this option in the My Devices portal.</td>
</tr>
<tr>
<td>Delete</td>
<td>For all devices. Enable employees to delete a registered device from the My Devices portal or to delete unused and add new devices, once the maximum number of registered devices is reached. This action removes the device from the list of devices displayed in the My Devices portal, but the device remains in the Cisco ISE database and continues to be listed in the Endpoints list. To define the maximum number of personal devices that employees can register using either the BYOD or My Devices portals, choose Administration &gt; Device Portal Management &gt; Settings &gt; Employee Registered Devices. To permanently delete the device from the Cisco ISE database, choose Work Centers &gt; Network Access &gt; Identities &gt; Endpoints.</td>
</tr>
<tr>
<td>Stolen</td>
<td>For all devices. Enable employees to indicate that their device is stolen. This action updates the device status in the My Devices portal to Stolen, adds the device to the Blacklist endpoint identity group, and removes its certificate.</td>
</tr>
<tr>
<td>Device lock</td>
<td>For MDM enrolled devices only. Enable employees to immediately lock their device remotely from the My Devices portal, in the event it is lost or stolen. This action prevents unauthorized use of the device. However, the PIN cannot be set in the My Devices portal and should have already been configured by the employee on their mobile device in advance.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unenroll</td>
</tr>
<tr>
<td>For MDM enrolled devices only. Enable employees to choose this option if they no longer need to use their device at work. This action removes only those applications and settings installed by your company, while retaining other apps and data on the employee's mobile device.</td>
</tr>
<tr>
<td>Full wipe</td>
</tr>
<tr>
<td>For MDM enrolled devices only. Enable employees to choose this option if they have lost their device or are replacing it with a new one. This action resets the employee's mobile device to its default factory settings, removing installed apps and data.</td>
</tr>
</tbody>
</table>

### Related Topics
- Manage Personal Devices Added by Employees, on page 516
  - My Devices Portal, on page 499

### Add, Edit, and Locate Device Customization for My Devices Portals

The navigation path for these settings are Administration > Device Portal Management > My Devices Portals > Create, Edit or Duplicate > Portal Page Customization > Add Devices, Edit Devices or Locate Devices.

Under Page Customizations, you can customize the messages, titles, content, instructions, and field and button labels that appear on the Add, Edit and Locate tabs of the My Devices portal.

### Related Topics
- My Devices Portal, on page 499
  - Create a My Devices Portal, on page 514

### Support Information Page Settings for Device Portals

The navigation path for this page is Administration > Device Portal Management > BYOD Portals, Client Provisioning Portals, MDM Portals, or My Devices Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Support Information Page Settings.

Use these settings to display the information that your Help Desk can use to troubleshoot access issues experienced by users (guests, sponsors or employees as applicable).

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include a Support Information Page</td>
<td>Display a link to an information page, such as Contact Us, on all enabled pages for the portal.</td>
</tr>
<tr>
<td>MAC address</td>
<td>Include the MAC address of the device on the Support Information page.</td>
</tr>
<tr>
<td>IP address</td>
<td>Include the IP address of the device on the Support Information page.</td>
</tr>
<tr>
<td>Field</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Browser user agent</td>
<td>Include the browser details such as the product name and version, layout engine and version of the user agent originating the request on the Support Information page.</td>
</tr>
<tr>
<td>Policy server</td>
<td>Include the IP address of the ISE Policy Service Node (PSN) that is serving this portal on the Support Information page.</td>
</tr>
<tr>
<td>Failure code</td>
<td>If available, include the corresponding number from the log message catalog. You can access and view the message catalog by navigating to Administration &gt; System &gt; Logging &gt; Message Catalog.</td>
</tr>
<tr>
<td>Hide field</td>
<td>Do not display any field labels on the Support Information page if the information that they would contain is non-existent. For example, if the failure code is unknown, and therefore blank, do not display Failure code, even if it is selected.</td>
</tr>
<tr>
<td>Display label with no value</td>
<td>Display all selected field labels on the Support Information page, even if the information that they would contain is non-existent. For example, if the failure code is unknown, display Failure code, even if it is blank.</td>
</tr>
<tr>
<td>Display label with default value</td>
<td>Display this text in any selected field on the Support Information page, if the information that they would contain is non-existent. For example, if you enter Not Available in this field, and the failure code is unknown, the Failure code displays Not Available.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Monitor My Devices Portals and Endpoints Activity, on page 517
- Access Device Portals, on page 497
CHAPTER 31

Guest Access User Interface Reference

- Guest Portal Settings, on page 1035
- Sponsor Portal Application Settings, on page 1051
- Global Settings, on page 1057

Guest Portal Settings

Portal Identification Settings

The navigation path for these settings is Work Centers > Guest Access > Portals & Components > Guest Portals or Sponsor Portals > Create, Edit or Duplicate > Guest Portals or Sponsor Portals Settings and Customization.

- **Portal Name**—Enter a unique portal name to access this portal. Do not use this portal name for any other Sponsor and Guest portals and non-guest portals, such as Blacklist, Bring Your Own Device (BYOD), Client Provisioning, Mobile Device Management (MDM), or My Devices portals.

  This name appears in the authorization profile portal selection for redirection choices, and is used in the list of portals for easy identification among other portals.

- **Description**—Optional.

- **Portal test URL**—A system-generated URL displays as a link after you click Save. Use it to test the portal.

  Click the link to open a new browser tab that displays the URL for this portal. In order for this to work, Policy Services Node (PSN) with Policy Services must be turned on. If Policy Services are not turned on, the PSN only displays the Admin portal.

  **Note** The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. For example, a redirect to an external URL will not work.

- **Language File**—Each portal type supports 15 languages by default, which are available as individual properties files bundled together in a single zipped language file. Export or import the zipped language
file to use with the portal. The zipped language file contains all the individual language files that you can use to display text for the portal.

The language file contains the mapping to the particular browser locale setting (for example, for French: fr, fr-fr, fr-ca) along with all of the string settings for the entire portal in that language. A single language file contains all the supported languages, so that it can easily be used for translation and localization purposes.

If you change the browser locale setting for one language, the change is applied to all the other end-user web portals. For example, if you change the French.properties browser locale from fr,fr-fr,fr-ca to fr,fr-fr in the Hotspot Guest portal, the change is applied to the My Devices portal also.

An alert icon displays when you customize any of the portal page text on the Portal Page Customizations tab. The alert message reminds you to update any changes made to one language while customizing the portal into all the supported languages properties files. You can manually dismiss the alert icon using the drop-down list option; or it is automatically dismissed after you import the updated zipped language file.

Portal Settings for Hotspot Guest Portals

The navigation path for these settings is Work Centers > Guest Access > Portals & Components > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Portal Settings.

- **HTTPS port**—Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you modify this page. If you modify this page, update the port setting to comply with this restriction.

If you assign Ports used by a non-guest (such as My Devices) portal to a guest portal, an error message displays.

For posture assessments and remediation only, the Client Provisioning portal also uses Ports 8905 and 8909. Otherwise, it uses the same Ports assigned to the Guest portal.

Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

- **Valid combinations include, using the Sponsor portal as an example:**
  - Sponsor portal: Port 8443, Interface 0, Certificate tag A and My Devices portal: Port 8443, Interface 0, Certificate group A.
  - Sponsor portal: Port 8443, Interface 0, Certificate group A and My Devices portal: Port 8445, Interface 0, Certificate group B.
  - Sponsor portal: Port 8444, Interface 1, Certificate group A and Blacklist portal: Port 8444, Interface 0, Certificate group B.

- **Invalid combinations include:**
  - Sponsor portal: Port 8443, Interface 0, Certificate group A and My Devices portal: 8443, Interface 0, Certificate group B.
  - Sponsor portal: Port 8444, Interface 0, Certificate tag A and Blacklist portal: Port 8444, Interface 0, Certificate group A.
• **Allowed interfaces** — Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed Port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets.

These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.

  • The Ethernet interfaces must use IP addresses on different subnets.
  
  • The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  
  • The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP.
  
  • Configure `ip host x.x.x.x yyy.domain.com` in ISE CLI to map secondary interface IP to FQDN, which is used to match Certificate Subject Name / Alternate Subject Name.
  
  • If only the bonded NIC is selected - When the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN logs an error and exits. The PSN will NOT try to start the portal on the physical interface.
  
  • **NIC teaming** or bonding is an O/S configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based on the portal settings configuration:
    
    • If both physical NICs and the corresponding bonded NIC are configured - When the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.
  
• **Certificate group tag**—Pick a certificate group tag that specifies the certificate to use for the portal’s HTTPS traffic.

• **Endpoint identity group**—Choose an endpoint identity group to track guest devices. Cisco ISE provides the GuestEndpoints endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

Choose an endpoint identity group to track employee devices. Cisco ISE provides the RegisteredDevices endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

• **Purge endpoints in this identity group when they reach ___ days**—Change the number of days since the registration of a user’s device before it is purged from the Cisco ISE database. Purging is done on a daily basis and the purge activity is synchronized with the overall purge timing. The change is applied globally for this endpoint identity group.

If changes are made to the Endpoint Purge Policy based on other policy conditions, this setting is no longer available for use.

• **Display Language**
Acceptable Use Policy (AUP) Page Settings for Hotspot Guest Portals

The navigation path for this page is **Work Centers > Guest Access > Portals & Components > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Acceptable Use Policy (AUP) Page Settings**

- **Include an AUP page**—Display your company’s network-usage terms and conditions on a separate page to the user.

- **Require an access code**—Assign an access code as the login credential that multiple guests should use to gain access to the network. An access code is primarily a locally known code that is given to physically present guests (either visually via a whiteboard or verbally by a lobby ambassador). It would not be known and used by someone outside the premises to access the network.

  You can use this option in addition to the usernames and passwords that are provided as the login credentials to individual guests.

- **Require scrolling to end of AUP**—Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP. Configure when the AUP appears to the user.

### Post-Access Banner Page Settings for Hotspot Portals

The navigation path for this page is **Work Centers > Guest Access > Portals & Components > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Post-Access Banner Page Settings**

Use this setting to inform guests of their access status and any other additional actions, if required.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include a Post-Access Banner page</td>
<td>Display additional information after the guests are successfully authenticated and before they are granted network access.</td>
</tr>
</tbody>
</table>
Portal Settings for Credentialed Guest Portals

The navigation path for these settings is: Work Centers > Guest Access > Portals & Components > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Portal Settings.

- **HTTPS port**—Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you modify this page. If you modify this page, update the port setting to comply with this restriction.

  If you assign Ports used by a non-guest (such as My Devices) portal to a guest portal, an error message displays.

  For posture assessments and remediation only, the Client Provisioning portal also uses Ports 8905 and 8909. Otherwise, it uses the same Ports assigned to the Guest portal.

  Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

  - **Valid combinations include**, using the Sponsor portal as an example:
    - Sponsor portal: Port 8443, Interface 0, Certificate tag A and My Devices portal: Port 8443, Interface 0, Certificate group A.
    - Sponsor portal: Port 8443, Interface 0, Certificate group A and My Devices portal: Port 8445, Interface 0, Certificate group B.
    - Sponsor portal: Port 8444, Interface 1, Certificate group A and Blacklist portal: Port 8444, Interface 0, Certificate group B.

  - **Invalid combinations include**:
    - Sponsor portal: Port 8443, Interface 0, Certificate group A and My Devices portal: 8443, Interface 0, Certificate group B.
    - Sponsor portal: Port 8444, Interface 0, Certificate tag A and Blacklist portal: Port 8444, Interface 0, Certificate group A.

- **Allowed interfaces** — Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed Port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets.

  These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.

  - The Ethernet interfaces must use IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  - The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP.
  - Configure `ip host x.x.x.x yyy.domain.com` in ISE CLI to map secondary interface IP to FQDN, which is used to match Certificate Subject Name / Alternate Subject Name.
• If only the bonded NIC is selected - When the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN logs an error and exits. The PSN will NOT try to start the portal on the physical interface.

• NIC teaming or bonding is an O/S configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based on the portal settings configuration:
  • If both physical NICs and the corresponding bonded NIC are configured - When the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

• The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP.

• Authentication Method — Choose which identity source sequence (ISS) or Identity Provider (IdP) to use for user authentication. The ISS is a list of Identity Stores that are searched in sequence to verify user credentials. Some examples include: Internal Guest Users, Internal Users, Active Directory, LDAP Directory.

Cisco ISE includes a default sponsor Identity Source Sequence for sponsor portals, Sponsor_Portal_Sequence.

To configure IdP, choose Administration > Identity Management > External Identity Sources > SAML Id Providers.

To configure an Identity Source Sequence, choose Administration > Identity Management > Identity Source Sequences.

• Employees using this portal as guests inherit login options from — Choose the Guest Type that employees are assigned when they log on to this portal. The employee's endpoint data is stored in the endpoint identity group configured in that guest type for the attribute Store device information in endpoint identity group. No other attributes from the associated guest type are inherited.

• Display Language
  • Use browser locale — Use the language specified in the client browser's locale setting as the display language of the portal. If browser locale's language is not supported by ISE, then the Fallback Language is used as the language portal.

  • Fallback language — Choose the language to use when language cannot be obtained from the browser locale, or if the browser locale language is not supported by ISE.

  • Always use — Choose the display language to use for the portal. This setting overrides the User browser locale option.

SSIDs available to sponsors — Enter the names or the SSIDs (Session Service Identifiers) of the networks that a sponsor can notify guests as the correct networks to connect to for their visit.
Login Page Settings for Credentialed Guest Portals

The navigation path for this page is: Work Centers > Guest Access > Portals & Components > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Login Page Settings

- **Require an access code**—Assign an access code as the login credential that multiple guests should use to gain access to the network. An access code is primarily a locally known code that is given to physically present guests (either visually via a whiteboard or verbally by a lobby ambassador). It would not be known and used by someone outside the premises to access the network.

  You can use this option in addition to the usernames and passwords that are provided as the login credentials to individual guests.

- **Maximum failed login attempts before rate limiting**—Specify the number of failed login attempts from a single browser session before Cisco ISE starts to throttle that account. This does not cause an account lockout. The throttled rate is configured in **Time between login attempts when rate limiting**.

- **Time between login attempts when rate limiting**—Set the length of time in minutes that a user must wait before attempting to log in again (throttled rate), after failing to log in the number of times defined in **Maximum failed login attempts before rate limiting**.

- **Include an AUP**—Add a acceptable use policy page to the flow. You can add the AUP to the page, or link to another page. Adding this changes the picture of the flow on the right.
  - **require acceptance**—Force the user to agree to the AUP before continuing the flow.

- **Allow guests to create their own accounts**—Provide an option on this portal’s Login page for guests to register themselves. If this option is not selected, sponsors create guest accounts. Enabling this also enables tabs on this page for you to configure **Self-Registration Page Settings** and **Self-Registration Success Page Settings**.

  If guests choose this option, they are presented with the Self-Registration form where they can enter the requested information to create their own guest accounts.

- **Allow Social Login**—Use a social media site to get login credentials for users of this portal. Checking this option displays the following settings:
  - **Show registration form after social login**—This allows the user to change the information provided by Facebook.
  - **Require guests to be approved**—This informs the user that a sponsor must approve their account, and will send them credentials for login.

- **Allow guests to change password after login**—Allow guests to change their password after successfully authenticating and accepting the AUP, if it is required. If guests change their passwords, sponsors cannot provide guests with their login credentials if lost. The sponsor can only reset the guest’s password back to a random password.

- **Allow the following identity-provider guest portal to be used for login**—Checking this option and selecting a SAML Id identity provider adds a link for that SAML Id to this portal. This sub-portal can be configured to look like the SAML IDP that the user is providing credentials for.

- **Allow social login**—All this portal to use a social media type for user login. Checking this item enables drop-downs to select the social media types you have configured. For more information about configuring social login, see **Social Login for Self-Registered Guests**, on page 456.
Self-Registration Page Settings

The navigation path for this page is **Work Centers > Guest Access > Portal & Components > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Self Registration Page Settings**. Use these settings to enable guests to register themselves and specify the information they must provide on the Self-Registration form.

- **Show guest form after social login**—This option skips the logon screen.

**Self-Registration Page Settings**

- **Assign self-registered guests to guest type**—Choose the guest type to which all the self-registered guests using this portal will be assigned.

- **Account valid for**—Specify the duration for the account in days, hours, or minutes after which the account expires unless you or the sponsor extend the account duration in the Sponsor portal.

- **Require a registration code for self registration**—Assign a code that the self-registering guests must enter to successfully submit their Self-Registration form. Similar to the access code, the registration code is provided to the guest offline to prevent someone who is outside the premises from accessing the system.

- **Fields to include**—On the self-registration page. Check the fields that you want to display on the Self-Registration form. Then check which fields are mandatory for the guests to complete in order to submit the form and receive a guest account. You may want to require fields such as SMS Service Provider and Person being Visited to gather important information from self-registering guests.

  - **Location**—Enter locations that the self-registering guests can select at registration time using the list of locations that you have defined. This automatically assigns the related time zones as the valid access times for these guests. The location names should be clear to avoid ambiguity during selection (for example, Boston Office, 500 Park Ave New York, Singapore.)

    If you plan to restrict guest access by time of day, the time zone is used to determine that time. Unless all your time-access controlled guests are in the San Jose time zone, then create a time zone for your locale. If there is only one location, it is automatically assigned as the default location, and this field does not display in the portal for guests to view. Also, **Location** is disabled in the list of **Fields to include**.

  - **SMS Service Provider**—Select which SMS providers to display on the Self-Registration form to enable self-registering guests to choose their own SMS provider. You can then use the guest’s SMS service to send them SMS notifications, which minimize expenses for your company. If you only selected one SMS provider for the guest to use, this field will not display on the Self-Registration form.

  - **Person being visited**—This is a text field, so if you want to use it, instruct your guests what kind of information to enter into this field.

  - **Custom Fields**—Select the custom fields that you previously created to collect more data from the self-registering guests. Then check which fields are mandatory for the guests to complete in order to submit the Self-Registration form and receive a guest account. These fields are listed in alphabetical order by name. They are created on **Work Centers > Guest Access > Settings > Custom Fields** to add more custom fields.

  - **Include an AUP**—Display your company’s network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.
• **Require acceptance**—Ensure that the user has read the AUP completely. This configures an Accept button on the self-registration page. If AUP is configured as on page, then you can also configure the Accept button to be disabled until after the user has scrolled to the end of the AUP.

• **Only allow guests with an email address from**—Specify a whitelist of domains which the self-registering guests can use in **EmailAddress** to create email addresses; for example, cisco.com.

  If you leave this field blank, any email address is valid, except for domains listed in Do not allow guests with email address from.

• **Do not allow guests with an email address from**—Specify a blacklist of domains which the self-registering guests cannot use in **EmailAddress** to create email addresses; for example, czgtgj.com.

• **Require self-registered guests to be approved**—Specify that the self-registering guests using this portal require approval from a sponsor before receiving their guest credentials. Clicking this option displays more options for how sponsors approve a self-registered guest. For more information about this, see Self-Registered Account Approval by Email, on page 470.

• **Email approval request to**—If you select:
  • **sponsor email addresses listed below**, enter one or more email addresses of sponsors designated as approvers, or a mailer, to which ALL guest approval requests should be sent.
  • **person being visited**, then the field **Require sponsor to provide credentials for authentication** is displayed, and the **Required option in Fields to include** is enabled (if it was previously disabled). These fields are displayed on the Self-Registration form requesting this information from the self-registering guests.

• **Approve/Deny Link Settings**—This section allows you to configure:
  • **Links are valid for**—You can set an expiration period for the account approval links.
  • **Require sponsor to provide credentials for authentication**—Check this to force the sponsor to enter credentials to approve the account, even if it is not required by the configuration in this section. This field is only visible if **Require self-registered guests to be approved** is set to **person being visited**.
  • **Sponsor is matched to a Sponsor Portal to verify approval privileges**—Click **Details >** to select the portals that are searched to verify that the sponsor is a valid system user, a member of a sponsor group, and that the members of that group have authority to approve the account. Each sponsor portal has an identity source sequence, which is used to identify the sponsor. Portals are used in the order they are listed. The first portal in the list determines the style and customization used in the sponsor portal.

• **After registration submission, direct guest to**—Choose where the self-registered guest is directed after successfully registering.
  • **Self-Registration Success page**—Direct successfully self-registered guests to the Self-Registration Success page, which displays the fields and messages you have specified on **Self Registration Success Page Settings**.

  It may not be desirable to display all the information, because the system may be awaiting account approval (if enabled on this page) or delivering the login credentials to an email address or phone number based on the whitelisted and blacklisted domains specified on this page.
If you enabled **Allow guests to log in directly from the Self-Registration Success page** in **Self-Registration Success Page Settings**, successfully self-registered guests can log in directly from this page. If it is not enabled, they are directed to the portal's Login page after the Self-Registration Success page is displayed.

- **Login page with instructions about how to obtain login credentials**—Direct successfully self-registered guests back to the portal’s Login page and display a message, such as “Please wait for your guest credentials to be delivered either via email, SMS, or print format and proceed with logging in.”

  To customize the default message, click the **Portal Page Customization** tab and select **Self-Registration Page Settings**.

  The system may be awaiting account approval (if enabled on this page) or delivering the login credentials to an email address or phone number based on the whitelisted and blacklisted domains specified on this page.

- **URL**—Direct successfully self-registered guests to the specified URL while waiting for their account credentials to be delivered.

  The system may be awaiting account approval (if enabled on this page) or delivering the login credentials to an email address or phone number based on the whitelisted and blacklisted domains specified on this page.

- **Send credential notification automatically using:**
  - **Email**—Choose email as the option by which successfully self-registered guests receive their login credential information. If you choose this option, **Email address** becomes a required field in the list of **Fields to include** and you can no longer disable this option.
  - **SMS**—Choose SMS as the option by which successfully self-registered guests receive their login credential information. If you choose this option, **SMS Service Provider** becomes a required field in the list of **Fields to include** and you can no longer disable this option.

### Self Registration Success Page Settings

The navigation path for this page is **Work Centers > Guest Access > Portals & Components > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Self Registration Success Page Settings**. Use these settings to notify successfully self-registered guests of the credentials they need to gain access to the network.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include this information on the Self-Registration Success page</td>
<td>Check the fields that you want to display for the successfully self-registered guests on the Self-Registration Success page. If sponsor approval of the guest is not required, check <strong>Username</strong> and <strong>Password</strong> to display these credentials for the guest. If sponsor approval is required, these fields are disabled, because the credentials can only be delivered to the guest after they have been approved.</td>
</tr>
<tr>
<td>Field</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>-------</td>
<td>------------------</td>
</tr>
<tr>
<td>Allow guest to send information to self using</td>
<td>Check the options by which the successfully self-registered guest can send credential information to themselves: Print, Email, or SMS.</td>
</tr>
<tr>
<td>Include an AUP (on page/as link)</td>
<td>Display your company’s network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.</td>
</tr>
<tr>
<td>Require acceptance</td>
<td>Require users to accept an AUP before their account is fully enabled. The Login button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not obtain network access.</td>
</tr>
<tr>
<td>Require scrolling to end of AUP</td>
<td>This field displays if you chose the AUP on page option. Ensure that the user has read the AUP completely. The Accept button activates only after the user has scrolled to the end of the AUP.</td>
</tr>
<tr>
<td>Allow guests to log in directly from the Self-Registration Success page</td>
<td>Display a Login button at the bottom of the Self-Registration Success page. This enables the guest to bypass the Login page and automatically deliver the login credentials to the portal and display the next page in the portal flow (for instance, the AUP page).</td>
</tr>
</tbody>
</table>

### Acceptable Use Policy (AUP) Page Settings for Credentialed Guest Portals

The navigation path for this page is **Work Centers > Guest Access > Portals & Components > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Acceptable Use Policy (AUP) Page Settings.**

- **Include an AUP page**—Display your company’s network-usage terms and conditions on a separate page to the user.

- **Use different AUP for employees**—Display a different AUP and network-usage terms and conditions for employees only. If you choose this option, you cannot also choose Skip AUP for employees.

- **Skip AUP for employees**—Employees are not required to accept an AUP before accessing the network. If you choose this option, you cannot also choose Use different AUP for employees.

- **Require scrolling to end of AUP**—This option displays only if Include an AUP on page is enabled. Ensure that the user has read the AUP completely. The Accept button activates only after the user has scrolled to the end of the AUP. Configure when the AUP appears to the user.

  - **On first login only**—Display an AUP the first time the user logs into the network or portal.

  - **On every login**—Display an AUP every time the user logs into the network or portal.

  - **Every ___ days (starting at first login)**—Display an AUP periodically after the user first logs into the network or portal.
Guest Change Password Settings for Credentialed Guest Portals

**Guest Change Password Settings**

The navigation path for this page is Work Centers > Guest Access > Portals & Components > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Guest Change Password Settings

- **Allow guests to change password after login**—Allow guests to change their password after successfully authenticating and accepting the AUP, if it is required. If guests change their passwords, sponsors cannot provide guests with their login credentials if lost. The sponsor can only reset the guest’s password back to a random password.

Guest Device Registration Settings for Credentialed Guest Portals

**Guest Device Registration Settings**

The navigation path for this page is Work Centers > Guest Access > Portals & Components > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Guest Device Registration Settings

Use these settings to either ensure that Cisco ISE automatically registers guest devices when they log in to or to allow guests to manually register their devices after they log in.

The maximum number of devices is specified for each guest type in Work Centers > Guest Access > Portals & Components > Guest Types.

- **Automatically register guest devices**—Automatically create an endpoint for the device from which the guest is accessing this portal. The endpoint is added to the endpoint identity group specified for this portal.
  
  An authorization rule can now be created to allow access to endpoints in that identity group, so that web authentication is no longer required.
  
  If the maximum number of registered devices is reached, the system automatically deletes the first registered device, registers the device the guest is trying to log in with, and notifies them. Choose Work Centers > Guest Access > Portals & Components > Guest Types to change the maximum number of devices with which a guest can register.

- **Allow guests to register devices**—Guests can register their devices manually by providing a name, description and MAC address. The MAC address is associated with an endpoint identity group.
  
  If the maximum number of registered devices is reached, the guest is required to delete at least one device before being allowed to register another device.

BYOD Settings for Credentialed Guest Portals

The navigation path for this page is Work Centers > Guest Access > Portals & Components > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > BYOD Settings.
Use these settings to enable Bring Your Own Device (BYOD) functionality for non-guests, such as employees, using the Credentialed Guest portals to access your corporate network.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow employees to use personal devices on the network</td>
<td>Add the Employee Bring Your Own Device (BYOD) Registration page to this portal allowing employees to go through the employee device registration process, and possibly native supplicant and certificate provisioning, depending on the settings for Client Provisioning for the employee’s personal device type (for example, iOS, Android, Windows (excluding RT or mobile), OSX).</td>
</tr>
<tr>
<td>Endpoint identity group</td>
<td>Choose an endpoint identity group to track guest devices. Cisco ISE provides the <strong>GuestEndpoints</strong> endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.</td>
</tr>
<tr>
<td>Allow employees to choose to get guest access only</td>
<td>Let employees access your guest network and avoid additional provisioning and registration that may be required to access your corporate network.</td>
</tr>
<tr>
<td>Display Device ID field during registration</td>
<td>Display the device ID to the user during the registration process, even though the device ID is pre-configured and cannot be changed while using the BYOD portal.</td>
</tr>
<tr>
<td>Originating URL</td>
<td>After successfully authenticating to the network, redirect the user’s browser to the original website that the user is trying to access, if available. If not available, the Authentication Success page displays. Make sure that the redirect URL is allowed to work on port 8443 of the PSN by the access-control list on the NAD and by authorization profiles configured in ISE for that NAD. For Windows, MAC and Android devices, control is given to the Self-Provisioning Wizard app, which does provisioning. Therefore, these devices are not redirected to the originating URL. However, iOS (dot1X) and unsupported devices (that are allowed network access) are redirected to this URL.</td>
</tr>
<tr>
<td>Success page</td>
<td>Display a page indicating that the device registration was successful.</td>
</tr>
<tr>
<td>URL</td>
<td>After successfully authenticating to the network, redirect the user's browser to the specified URL, such as your company’s website.</td>
</tr>
</tbody>
</table>
Post-Login Banner Page Settings for Credentialed Guest Portals

The navigation path for this page is Work Centers > Guest Access > Portals & Components > Guest Portals or Sponsor Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Post-Login Banner Page Settings.

Use this setting to notify users (guests, sponsors or employees as applicable) of additional information after they log in successfully.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include a Post-Login Banner page</td>
<td>Display additional information after the users successfully log in and before they are granted network access.</td>
</tr>
</tbody>
</table>

Guest Device Compliance Settings for Credentialed Guest Portals

The navigation path for this page is Work Centers > Guest Access > Portals & Components > Guest Portals or Sponsor Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Guest Device Compliance Settings. Use these settings to require guests, and employees using the guest portal, to undergo client provisioning of their devices in order to gain access to the network.

- **Require guest device compliance**—Redirect guests to the Client Provisioning page, which requires them to download a posture agent. This adds client provisioning to the Guest flow, where you configure posture policies for guests, such as checking for virus protection software.

  If the guest is an employee using the Credentialed Guest portals to access the network and:

  - If you enabled *Allow employees to use personal devices on the network* in the BYOD Settings, the employee is redirected to the BYOD flow and will not undergo client provisioning.

  - If you enabled both *Allow employees to use personal devices on the network* and *Allow employees to choose to get guest access only* in the BYOD Settings, and the employee chooses guest access, they are routed to the Client Provisioning page.

VLAN DHCP Release Page Settings for Guest Portals

The navigation path for this page is Work Centers > Guest Access > Portals & Components > Guest Portals or Sponsor Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > VLAN DHCP Release Page Settings.

- **Enable VLAN DHCP release**—Refresh a guest's IP address for Windows and Mac OS devices after a VLAN change in both wired and wireless environments.

  This affects the Central WebAuth (CWA) flow during final authorization, when the network access changes the guest VLAN to a new VLAN. The guest's old IP address must be released before the VLAN change, and a new guest IP address must be requested through DHCP when the guest connects to the new VLAN. The IP address release renew operation varies by the browser and operating system used; Internet Explorer uses ActiveX controls, and Firefox and Google Chrome use Java applets. For non-Internet Explorer browsers, Java must be installed and enabled on the browser.
The VLAN DHCP Release option does not work on mobile devices. Instead, guests are requested to manually reset the IP address. This method varies by devices. For example, on Apple iOS devices, guests can select the Wi-Fi network and click the Renew Lease button.

- **Delay to release __ seconds**—Enter the delay to release time. We recommend a short value, because the release must occur immediately after the applet is downloaded, and before the Cisco ISE server directs the NAD to re-authenticate with a CoA request.

- **Delay to CoA __ seconds**—Enter the time to delay Cisco ISE from executing the CoA. Provide enough time (use the default value as a guideline) to allow the applet to download and perform the IP release on the client.

- **Delay to renew __ seconds**—Enter the delay to renew value. This time is added to the IP release value and does not begin timing until the control is downloaded. Provide enough time (use the default value as a guideline) so that the CoA is allowed to process and the new VLAN access granted.

### Authentication Success Settings for Guest Portals

The navigation path for this page is Work Centers > Guest Access > Portals & Components > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Authentication Success Settings.

These settings notify the users (guests, sponsors, or employees as applicable) of authentication success or display a URL. Under **Once authenticated, take guest to**, configure the following fields:

- **Originating URL**—After successfully authenticating to the network, redirect the user’s browser to the original website that the user is trying to access, if available. If not available, the Authentication Success page displays. Make sure that the redirect URL is allowed to work on port 8443 of the PSN by the access-control list on the NAD and by authorization profiles configured in ISE for that NAD.

  For Windows, MAC and Android devices, control is given to the Self-Provisioning Wizard app, which does provisioning. Therefore, these devices are not redirected to the originating URL. However, iOS (dot1X) and unsupported devices (that are allowed network access) are redirected to this URL.

- **Authentication Success page**—Notification of successful authentication of the user.

- **URL**—After successfully authenticating to the network, redirect the user's browser to the specified URL, such as your company’s website.

---

**Note**

If you redirect a Guest to an external URL after authentication, there may be a delay while the URL address is resolved and the session is redirected. Make sure that the redirect URL is allowed to work on port 8443 of the PSN by the access-control list on the NAD and by authorization profiles configured in ISE for that NAD.

### Support Information Page Settings for Guest Portals

The navigation path for this page is Work Centers > Guest Access > Portals & Components > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Support Information Page Settings.
Use these settings to display the information that your Help Desk can use to troubleshoot access issues experienced by users (guests, sponsors or employees as applicable).

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include a Support Information Page</td>
<td>Display a link to an information page, such as Contact Us, on all enabled pages for the portal.</td>
</tr>
<tr>
<td>MAC address</td>
<td>Include the MAC address of the device on the Support Information page.</td>
</tr>
<tr>
<td>IP address</td>
<td>Include the IP address of the device on the Support Information page.</td>
</tr>
<tr>
<td>Browser user agent</td>
<td>Include the browser details such as the product name and version, layout engine and version of the user agent originating the request on the Support Information page.</td>
</tr>
<tr>
<td>Policy server</td>
<td>Include the IP address of the ISE Policy Service Node (PSN) that is serving this portal on the Support Information page.</td>
</tr>
<tr>
<td>Failure code</td>
<td>If available, include the corresponding number from the log message catalog. You can access and view the message catalog by navigating to Administration &gt; System &gt; Logging &gt; Message Catalog.</td>
</tr>
<tr>
<td>Hide field</td>
<td>Do not display any field labels on the Support Information page if the information that they would contain is non-existent. For example, if the failure code is unknown, and therefore blank, do not display Failure code, even if it is selected.</td>
</tr>
<tr>
<td>Display label with no value</td>
<td>Display all selected field labels on the Support Information page, even if the information that they would contain is non-existent. For example, if the failure code is unknown, display Failure code, even if it is blank.</td>
</tr>
<tr>
<td>Display label with default value</td>
<td>Display this text in any selected field on the Support Information page, if the information that they would contain is non-existent. For example, if you enter Not Available in this field, and the failure code is unknown, the Failure code displays Not Available.</td>
</tr>
</tbody>
</table>
Sponsor Portal Application Settings

Portal Identification Settings

The navigation path for these settings is Work Centers > Guest Access > Portals & Components > Guest Portals or Sponsor Portals > Create, Edit or Duplicate > Guest Portals or Sponsor Portals Settings and Customization.

- **Portal Name**—Enter a unique portal name to access this portal. Do not use this portal name for any other Sponsor and Guest portals and non-guest portals, such as Blacklist, Bring Your Own Device (BYOD), Client Provisioning, Mobile Device Management (MDM), or My Devices portals.

  This name appears in the authorization profile portal selection for redirection choices, and is used in the list of portals for easy identification among other portals.

- **Description**—Optional.

- **Portal test URL**—A system-generated URL displays as a link after you click Save. Use it to test the portal.

  Click the link to open a new browser tab that displays the URL for this portal. In order for this to work, Policy Services Node (PSN) with Policy Services must be turned on. If Policy Services are not turned on, the PSN only displays the Admin portal.

  **Note**  
  The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. For example, a redirect to an external URL will not work.

- **Language File**—Each portal type supports 15 languages by default, which are available as individual properties files bundled together in a single zipped language file. Export or import the zipped language file to use with the portal. The zipped language file contains all the individual language files that you can use to display text for the portal.

  The language file contains the mapping to the particular browser locale setting (for example, for French: fr, fr-fr, fr-ca) along with all of the string settings for the entire portal in that language. A single language file contains all the supported languages, so that it can easily be used for translation and localization purposes.

  If you change the browser locale setting for one language, the change is applied to all the other end-user web portals. For example, if you change the French.properties browser locale from fr,fr-fr,fr-ca to fr,fr-fr in the Hotspot Guest portal, the change is applied to the My Devices portal also.

  An alert icon displays when you customize any of the portal page text on the Portal Page Customizations tab. The alert message reminds you to update any changes made to one language while customizing the portal into all the supported languages properties files. You can manually dismiss the alert icon using the drop-down list option; or it is automatically dismissed after you import the updated zipped language file.
Portal Settings for Sponsor Portals

Configure these settings to identify the portal and select the language files to be used for all the portal pages.

- **HTTPS port** — Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you modify this page. If you modify this page, update the port setting to comply with this restriction.

If you assign Ports used by a non-guest (such as My Devices) portal to a guest portal, an error message displays.

For posture assessments and remediation only, the Client Provisioning portal also uses Ports 8905 and 8909. Otherwise, it uses the same Ports assigned to the Guest portal.

Portals assigned to the same HTTPS port can use the same Gigabit Ethernet interface or another interface. If they use the same port and interface combination, they must use the same certificate group tag. For example:

- **Valid combinations include**, using the Sponsor portal as an example:
  - Sponsor portal: Port 8443, Interface 0, Certificate tag A and My Devices portal: Port 8443, Interface 0, Certificate group A.
  - Sponsor portal: Port 8443, Interface 0, Certificate group A and My Devices portal: Port 8445, Interface 0, Certificate group B.
  - Sponsor portal: Port 8444, Interface 1, Certificate group A and Blacklist portal: Port 8444, Interface 0, Certificate group B.

- **Invalid combinations include**:
  - Sponsor portal: Port 8443, Interface 0, Certificate group A and My Devices portal: 8443, Interface 0, Certificate group B.
  - Sponsor portal: Port 8444, Interface 0, Certificate tag A and Blacklist portal: Port 8444, Interface 0, Certificate group A.

- **Allowed interfaces** — Select the PSN interfaces which a PAN can use to run a portal. When a request to open a portal is made on the PAN, the PAN looks for an available allowed Port on the PSN. You must configure the Ethernet interfaces using IP addresses on different subnets.

These interfaces must be available on all the PSNs, including VM-based ones, that have Policy Services turned on. This is a requirement because any of these PSNs can be used for the redirect at the start of the guest session.

- The Ethernet interfaces must use IP addresses on different subnets.
- The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
- The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP.
- Configure `ip host x.x.x.x yyyy.domain.com` in ISE CLI to map secondary interface IP to FQDN, which is used to match Certificate Subject Name / Alternate Subject Name.
• If only the bonded NIC is selected - When the PSN attempts to configure the portal it first attempts to configure the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN logs an error and exits. The PSN will NOT try to start the portal on the physical interface.

• **NIC teaming** or bonding is an O/S configuration option that allows you to configure two individual NICs for high availability (fault tolerance). If one of the NICs fails, the other NIC that is part of the bonded connection continues the connection. A NIC is selected for a portal based on the portal settings configuration:
  - If both physical NICs and the corresponding bonded NIC are configured - When the PSN attempts to configure the portal, it first attempts to connect to the Bond interface. If that is not successful, perhaps because there was no bond setup on that PSN, then the PSN attempts to start the portal on the physical interface.

• **Certificate group tag**—Pick a certificate group tag that specifies the certificate to use for the portal’s HTTPS traffic.

• **Fully Qualified Domain Name (FQDN)**—Enter at least one unique FQDN and/or hostname for your Sponsor or MyDevices portal. For example, you can enter `sponsorportal.yourcompany.com`, so that when the user enters either of those into a browser, the sponsor portal displays. Separate names with commas, but do not include spaces between entries.

If you change the default FQDN, then also do the following:

- Update your DNS so that the FQDN of the new URL resolves to a valid Policy Services Node (PSN) IP address. Optionally, this address could point to a load balancer virtual IP address that serves a pool of PSNs.

- To avoid certificate warning messages due to name mismatches, include the FQDN of the customized URL, or a wildcard, in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE PSN.

• **Authentication Method** —Choose which identity source sequence (ISS) or Identity Provider (IdP) to use for user authentication. The ISS is a list of Identity Stores that are searched in sequence to verify user credentials. Some examples include: Internal Guest Users, Internal Users, Active Directory, LDAP Directory.

Cisco ISE includes a default sponsor Identity Source Sequence for sponsor portals, Sponsor_Portal_Sequence.

To configure IdP, choose Administration > Identity Management > External Identity Sources > SAML Id Providers.

To configure an Identity Source Sequence, choose Administration > Identity Management > Identity Source Sequences.

• **Idle timeout**—Enter the time in minutes that you want Cisco ISE to wait before it logs out the user if there is no activity in the portal. The valid range is from 1 to 30 minutes.

• **Allow Kerberos**—Use Kerberos to authenticate a sponsor for access to the sponsor portal. Kerberos SSO is performed inside the secure tunnel after the browser establishes the SSL connection with ISE.
Kerberos authentication requires the following items to be in the same domain:

- Sponsor's PC
- ISE PSN
- FQDN configured for this sponsor portal

Note
Kerberos authentication is NOT supported for the Guest portal.

- Display Language
  - Use browser locale—Use the language specified in the client browser's locale setting as the display language of the portal. If browser locale's language is not supported by ISE, then the Fallback Language is used as the language portal.

  - Fallback language—Choose the language to use when language cannot be obtained from the browser locale, or if the browser locale language is not supported by ISE.

  - Always use—Choose the display language to use for the portal. This setting overrides the User browser locale option.

SSIDs available to sponsors—Enter the names or the SSIDs (Session Service Identifiers) of the networks that a sponsor can notify guests as the correct networks to connect to for their visit.

- SSIDs available to sponsors—Enter the names or the SSIDs (Session Service Identifiers) of the networks that a sponsor can notify guests as the correct networks to connect to for their visit.

## Login Settings for Sponsor Portals

### Login Page Settings for Sponsor Portals

The navigation path for this page is Work Centers > Guest Access > Portals & Components > Sponsor Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Login Page Settings

- Maximum failed login attempts before rate limiting—Specify the number of failed login attempts from a single browser session before Cisco ISE starts to throttle that account. This does not cause an account lockout. The throttled rate is configured in Time between login attempts when rate limiting.

- Time between login attempts when rate limiting—Set the length of time in minutes that a user must wait before attempting to log in again (throttled rate), after failing to log in the number of times defined in Maximum failed login attempts before rate limiting.

- Include an AUP—Add a acceptable use policy page to the flow. You can add the AUP to the page, or link to another page. Adding this changes the picture of the flow on the right.
  - require acceptance—Force the user to agree to the AUP before continuing the flow.
Acceptable Use Policy (AUP) Settings for Sponsor Portals

The navigation path for this page is Work Centers > Guest Access > Portals & Components > Sponsor Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Acceptable Use Policy (AUP) Page Settings.

Use these settings to define the AUP experience for the users (guests, sponsors or employees as applicable).

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include an AUP page</td>
<td>Display your company’s network-usage terms and conditions on a separate page to the user.</td>
</tr>
<tr>
<td>Require scrolling to end of AUP</td>
<td>Ensure that the user has read the AUP completely. The Accept button activates only after the user has scrolled to the end of the AUP.</td>
</tr>
<tr>
<td>On first login only</td>
<td>Display an AUP when the user logs into the network or portal for the first time only.</td>
</tr>
<tr>
<td>On every login</td>
<td>Display an AUP each time the user logs into the network or portal.</td>
</tr>
<tr>
<td>Every ___ days (starting at first login)</td>
<td>Display an AUP periodically after the user first logs into the network or portal.</td>
</tr>
</tbody>
</table>

Sponsor Change Password Settings for Sponsor Portals

The navigation path for this page is Work Centers > Guest Access > Portals & Components > Sponsor Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Sponsor Change Password Settings. Use these settings to define the password requirements for sponsors using the Sponsor portal.

To set the sponsor password policy, choose Administration > Identity Management > Settings > User Password Policy.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow sponsors to change their own passwords</td>
<td>Allow sponsors to change their passwords after they log into the Sponsor portal. This option will display a Change Password page only if the sponsors are part of the Internal Users database.</td>
</tr>
</tbody>
</table>

Post-Login Banner Settings for Sponsor Portals

The navigation path for this page is Work Centers > Guest Access > Portals & Components > Guest Portals or Sponsor Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Post-Login Banner Page Settings.
Use this setting to notify users (guests, sponsors or employees as applicable) of additional information after they log in successfully.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include a Post-Login Banner page</td>
<td>Display additional information after the users successfully log in and before they are granted network access.</td>
</tr>
</tbody>
</table>

## Support Information Page Settings for Sponsor Portals

The navigation path for this page is **Work Centers > Guest Access > Portals & Components > Sponsor Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Support Information Page Settings.**

Use these settings to display the information that your Help Desk can use to troubleshoot access issues experienced by users (guests, sponsors or employees as applicable).

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include a Support Information Page</td>
<td>Display a link to an information page, such as Contact Us, on all enabled pages for the portal.</td>
</tr>
<tr>
<td>MAC address</td>
<td>Include the MAC address of the device on the Support Information page.</td>
</tr>
<tr>
<td>IP address</td>
<td>Include the IP address of the device on the Support Information page.</td>
</tr>
<tr>
<td>Browser user agent</td>
<td>Include the browser details such as the product name and version, layout engine and version of the user agent originating the request on the Support Information page.</td>
</tr>
<tr>
<td>Policy server</td>
<td>Include the IP address of the ISE Policy Service Node (PSN) that is serving this portal on the Support Information page.</td>
</tr>
<tr>
<td>Failure code</td>
<td>If available, include the corresponding number from the log message catalog. You can access and view the message catalog by navigating to Administration &gt; System &gt; Logging &gt; Message Catalog.</td>
</tr>
<tr>
<td>Hide field</td>
<td>Do not display any field labels on the Support Information page if the information that they would contain is non-existent. For example, if the failure code is unknown, and therefore blank, do not display Failure code, even if it is selected.</td>
</tr>
</tbody>
</table>
### Notify Guests Customization for Sponsor Portals

The navigation path for these settings is **Work Centers > Guest Access > Portals & Components > Sponsor Portals > Create, Edit or Duplicate > Portal Page Customization > Notify Guests.**

Under **Page Customizations**, you can customize the messages, titles, content, instructions, and field and button labels that appear on the notifications that sponsors send to guests from the Sponsor portal.

Under **Settings**, you can specify whether sponsors can send usernames and passwords separately to guests using email or SMS. You can also specify whether sponsors can display a Support Information page for guests to provide information that a help desk can use to troubleshoot access issues.

### Manage and Approve Customization for Sponsor Portals

The navigation path for these settings is **Work Centers > Guest Access > Portals & Components > Sponsor Portals > Create, Edit or Duplicate > Portal Page Customization > Manage and Approve.**

Under **Page Customizations**, you can customize the messages, titles, content, instructions, and field and button labels that appear on the Manage and Approve tabs of the Sponsor portal.

These include the accounts (registered and pending) summary and detailed views, the pop-up dialogs that display based on the operations the sponsor performs on guest accounts such as edit, extend, suspend and so on, and also general portal and account action messages.

### Global Settings

#### Global Settings for Guest and Sponsor Portals

Choose **Guest Access > Settings.** You can configure the following general settings that apply to Guest and Sponsor portals, guest types, and sponsor groups in Cisco ISE:

- Policies for purging guest accounts and generating usernames and passwords.

- SMTP servers and SMS gateways to use when sending email and SMS notifications to guests and sponsors.
• Locations, time zones, SSIDs, and custom fields to select from when creating guest accounts and when registering guests using Self-Registration Guest portals.

Once you configure these global settings, you can use them as needed when configuring specific Guest and Sponsor portals, guest types, and sponsor groups.

The following tabs are on the Portal settings page:

• **Guest Account Purge Policy**—Schedule when to purge guest accounts that have expired. For more information, see Schedule When to Purge Expired Guest Accounts, on page 449.

• **Custom Fields**—Add custom fields to use in Guest portals, to retrieve additional information from users. For more information, see Add Custom Fields for Guest Account Creation, on page 450.

• **Guest Email Settings**—Decide whether to email notifications to guests about changes in their account. For more information, see Specify Email Addresses and SMTP Servers for Email Notifications, on page 450.

• **Guest Locations and SSIDs**—Configure the Locations and the Service Set Identifiers (SSIDs) of the networks that guests can use at these Locations. For more information, see Assign Guest Locations and SSIDs, on page 451.

• **Guest Username Policy**—Configure how guest user names are created. For more information, see Set the Guest Username Policy, on page 454 and Rules for Guest Password Policies, on page 452.

• **Guest Password Policy**—Define the guest password policies for all Guest and Sponsor portals. For more information, see Set the Guest Password Policy and Expiration, on page 453.

• **Logging**—Guest users are tracked by the MAC address of their device. When guest users are displayed in reports, the username is the MAC address. If you select this option, reports will show the portal user ID as the username, instead of the MAC address. For more information about this option, see Guest Remember Me, on page 474.

---

**Guest Type Settings**

The navigation path for these settings is Work Centers > Guest Access > Portals & Components > Guest Types. Use these settings to create the types of Guests that can access your network and their access privileges. You can also specify which Sponsor Groups can create this type of Guest.

• **Guest type name**—Provide a name (from 1 to 256 characters) that distinguishes this Guest Type from the other Guest Types.

• **Description**—Provide additional information (maximum of 2000 characters) about the recommended use of this Guest Type, for example, Use for self-registering Guests. Do not use for Guest account creation, and so forth.

• **Language File**—This field allows you to export and import the language file, which contains content for email subject, email message, and SMS messages in all supported languages. These languages and content are used in notifications about an expired account, and are sent to guests who are assigned to this guest type. If you are creating a new guest type, this feature is disabled until after you save the guest type. For more information about editing the language file, see Portal Language Customization, on page 548.

• **Collect Additional Data**—Click the Custom Fields... button to select which custom fields to use to collect additional data from guests using this Guest Type.
To manage custom fields, choose Work Centers > Guest Access > Settings > Custom Fields.

- **Maximum Access Time**
  - **Account duration starts**—If you select From first login, the account start time starts when the guest user first logs in to the guest portal, and the end time equals the configured duration time. If the guest user never logs in, the account remains in the Awaiting first login state until the guest account purge policy removes the account.

  Values are from 1 to 999 days, hours, or minutes.

  A self-registered user’s account starts when they create and log on to their account.

  If you select From sponsor-specified date, enter the maximum number of days, hours, or minutes that Guests of this Guest Type can access and stay connected to the network.

  If you change these settings, your changes will not apply to existing Guest accounts that were created using this Guest Type.

  - **Maximum account duration**—Enter the number of days, hours, or minutes that guests assigned to this guest type can log on.

  __Note__
  The account purge policy checks for expired guest accounts, and sends expiration notification. This policy runs every 20 minutes, so if you set the account duration to less than 20 mins, it is possible that expiration notices may not be sent out before the account is purged.

  You can specify the duration time and the days of the week when access is provided to the guests of this Guest Type by using the Allow access only on these days and times option.

  - The days of the week that you select limits access to the dates that are selectable in the Sponsor’s calendar.

  - Maximum account duration is enforced in the sponsor portal, when the Sponsor picks duration and dates.

  The settings you make here for access time affect the time settings that are available on the sponsor portal when creating a guest account. For more information, see Configuring the Time Settings Available to Sponsors, on page 484.

- **Logon Options**
  - **Maximum simultaneous logins**—Enter the maximum number of user sessions that users assigned to this Guest Type can have running concurrently.

  - **When guest exceeds limit**—When you select Maximum simultaneous logins, you must also select the action to take when a user connects after the maximum number of log ins is reached.

    - ** Disconnect the oldest connection**
    - ** Disconnect the newest connection**—Optionally select Redirect user to a portal page showing an error message: An error message is displayed for a configurable amount of time, then the session is disconnected, and the user is redirected to the Guest portal. The error page's content is configured on the Portal Page Customization dialog, on the Messages > Error Messages page.
• **Maximum devices guests can register**—Enter the maximum number of devices that can be registered to each Guest. You can set the limit to a number lower than what is already registered for the Guests of this Guest Type. This only affects newly created Guest accounts. When a new device is added, and the maximum is reached, the oldest device is disconnected.

• **Endpoint identity group for guest device registration**—Choose an endpoint identity group to assign to guest devices. Cisco ISE provides the **GuestEndpoints** endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

• **Allow guest to bypass the Guest portal**—Allows users to bypass the credentialed guest-type captive portal (web authentication page), and access the network by providing credentials to wired and wireless (dot1x) supplicants or VPN clients. Guest accounts change to the **Active** state, bypassing the **Awaiting Initial Login** state and the **AUP** page, even if the AUP is required.

If you do not enable this setting, users must first log in through the credentialed Guest captive portal before they are able to access other parts of the network.

• **Account Expiration Notification**
  
  • **Send account expiration notification ____ days before account expires**—Send a notification to Guests before their account expires and specify how many days, hours, or minutes before the expiration.
  
  • **View messages in**—Specify the language to use when displaying email or SMS notifications as you set them up.
  
  • **Email**—Send account expiration notices by email.
  
  • **Use customization from**—Apply the same customizations that you configured for the selected portal to this Guest Type's account expiration emails.
  
  • **Copy text from**—Reuse email text that you created for another Guest Type's account expiration email.
  
  • **Send test email to me at**
  
  • **SMS**—Send account expiration notices by SMS.

  The settings that follow for SMS are the same as for email notifications, except that you choose an SMS gateway for **Send test SMS to me**.

• **Sponsor Groups**—Specify the sponsor groups whose members can create a guest account using this guest type. Delete the sponsor groups that you do not want to have access to this guest type.

### Sponsor Group Settings

The navigation path for these settings is **Work Centers > Guest Access > Portals & Components > Sponsor Groups**. Use these settings to add members to the sponsor group, define guest types and location privileges, and set permissions related to creating and managing guest accounts.

• **Disable Sponsor Group**—Disable members of this sponsor group from accessing the Sponsor portal.

For instance, you may want to temporarily prevent sponsors from logging in to the Sponsor portal while configuration changes are being made in the Admin portal. Or, you may want to disable a sponsor group...
that is involved in infrequent activity, such as sponsoring guests for an annual convention, until the time they need to be activated again.

- **Sponsor group name**—Enter a unique name (from 1 to 256 characters).

- **Description**—Include useful information (maximum of 2000 characters) such as the guest types used by this sponsor group.

- **Configure Guest Types**—If the guest type you need is not available, click **Work Centers > Guest Access > Portals & Components > Guest Types** and create a new guest type or edit an existing one.

**Match Criteria**

- **Members**—Click to display the **Select Sponsor Group Members** box, where you can select available user identity groups (from internal and external identity stores) and add them as members of this sponsor group.

  - **Sponsor Group Members**—Search and filter the list of selected sponsor groups and delete any groups you do not want to include.

- **Other conditions**—Click **Create New Condition** to build one or more conditions that a sponsor must match to be included in this sponsor group. You can use authentication attributes from Active Directory, LDAP, SAML, and ODBC identity stores, but not RADIUS Token or RSA SecurID stores. You can also use internal user attributes. Conditions have an attribute, and operator, and a value.

  - To create a condition using the internal dictionary attribute **Name**, prefix the identity group name with User Identity Groups. For example:

    \[InternalUser:Name \text{EQUALS} \text{bsmith}\]

    This means that only internal users with the Name "bsmith" can belong to this sponsor group.

- **This sponsor group can create accounts using these guest types**—Specify the guest types that the members in this sponsor group can use when creating guest accounts. For a sponsor group to be enabled, it must have at least one guest type that it can use.

  If you assign only one guest type to this sponsor group, you can choose not to display it in the Sponsor portal since it is the only valid guest type available for use. Choose **Work Centers > Guest Access > Portals & Components > Sponsor Portal > Page Customization > Create Accounts > Guest Types > Settings**. Check **Hide guest type if only one is available to sponsor** to enable this option.

- **Select the locations that guests will be visiting**—Select the various locations sponsors in this group can assign to guests when creating their accounts. This helps define the valid time zones for these guest accounts and specifies all the time parameters that apply to the guest, such as valid access times, and so on. This does not prevent guests from connecting to the network from other locations.

  For a sponsor group to be enabled, it must have at least one location that it can use.

  If you assign only one location to this sponsor group, it will be the only valid time zone for the guest accounts created by its members. By default, it does not display in the Sponsor portal.

**Sponsor Can Create**

- **Multiple guest accounts assigned to specific guests (Import)**—Enable the sponsor to create multiple guest accounts by importing guest details such as first name and last name from a file.
If this option is enabled, the Import button displays in the Create Accounts page of the Sponsor portal. The Import option is only available on desktop browsers (not mobile), such as Internet Explorer, Firefox, Safari, and so forth.

- **Limit to batch of**—If this sponsor group is allowed to create multiple accounts simultaneously, specify the number of guest accounts that can be created in a single import operation.

Although a sponsor can create a maximum of 10,000 accounts, we recommend that you limit the number of accounts you create, due to potential performance issues.

- **Multiple guest accounts to be assigned to any guests (Random)**—Enable the sponsor to create multiple random guest accounts as placeholders for guests who are not known as yet, or when they need to create many accounts quickly.

If this option is enabled, the Random button displays on the Create Accounts page of the Sponsor portal.

- **Default username prefix**—Specify a username prefix that sponsors can use when creating multiple random guest accounts. If specified, this prefix appears in the Sponsor Portal when creating random guest accounts. In addition, if Allow sponsor to specify a username prefix is:
  - Enabled—The sponsor can edit the default prefix in the Sponsor portal.
  - Not enabled—The sponsor cannot edit the default prefix in the Sponsor portal.

If you do not specify a username prefix or allow the sponsor to specify one, then the sponsor will not be able to assign username prefixes in the Sponsor portal.

- **Allow sponsor to specify a username prefix**—If this sponsor group is allowed to create multiple accounts simultaneously, specify the number of guest accounts that can be created in a single import operation.

Although a sponsor can create a maximum of 10,000 accounts, we recommend that you limit the number of accounts you create, due to potential performance issues.

- **Start date can be no more than ___ days into the future**—Enable and specify the number of days within which sponsors have to set as the start date for the multiple guest accounts they have created.

**Sponsor Can Manage**

- **Only accounts sponsor has created**—Sponsors in this group can view and manage only the guest accounts that they have created, which is based on the Sponsor’s email account.

- **Accounts created by members of this sponsor group**—Sponsors in this group can view and manage the guest accounts created by any sponsor in this sponsor group.

- **All guest accounts**—Sponsors view and manage all pending guest accounts.

---

**Note**

Regardless of the group membership, all sponsors can see all pending accounts, unless you check Approve and view requests from self-registering guests with the option Only pending accounts assigned to this sponsor under Sponsor Can.
Sponsor Can

- **Update guests’ contact information (email, PhoneNumber)**—For guest accounts that they can manage, allow the sponsor to change a guest’s contact information.

- **View/print guests’ passwords**—When this is checked the sponsor can print passwords for guests. The sponsor can see the passwords for guests on the Manage Accounts page and in the details for a guest. When this is not checked, the sponsor can’t print the password, but the user can still get the password through email or SMS, if configured.

- **Send SMS notifications with guests’ credentials**—For guest accounts that they can manage, allow the sponsor to send SMS (text) notifications to guests with their account details and login credentials.

- **Reset guest account passwords**—For guest accounts that they can manage, allow the sponsor to reset passwords for guests to a random password generated by Cisco ISE.

- **Extend guests’ accounts**—For guest accounts that they can manage, allow the sponsor to extend them beyond their expiration date. The sponsor is automatically copied on email notifications sent to guests regarding their account expiration.

- **Delete guests’ accounts**—For guest accounts that they can manage, allow the sponsor to delete the accounts, and prevent guests from accessing your company's network.

- **Suspend guests’ accounts**—For guest accounts that they can manage, allow the sponsor to suspend their accounts to prevent guests from logging in temporarily. This action also issues a Change of Authorization (CoA) Terminate to remove the suspended guests from the network.

  - **Require sponsor to provide a reason**—Require the sponsor to provide an explanation for suspending the guest accounts.

- **Approve and view requests from self-registering guests**—Sponsors who are included in this Sponsor Group can either view all pending account requests from self-registering guests (that require approval), or only the requests where the user entered the Sponsor's email address as the person being visited. This feature requires that the portal used by the Self-registering guest has **Require self-registered guests to be approved** checked, and the Sponsor's email is listed as the person to contact.

  - Any pending accounts—A sponsor belonging to this group can approve and review accounts that were created by any sponsor.

  - Only pending accounts assigned to this sponsor—A sponsor belonging to this group can only view and approve accounts that they created.

- **Access Cisco ISE guest accounts using the programmatic interface (Guest REST API)**—For guest accounts that they can manage, allow the sponsor to access guest accounts using the Guest REST API programming interface.
Chapter 32

Web Portals Customization Reference

- Portal Pages Titles, Content and Labels Character Limits, on page 1065
- Portal Customization, on page 1067
- HTML Support for a Portal Language File, on page 1068

Portal Pages Titles, Content and Labels Character Limits

There is a maximum and minimum range of characters you can enter in the titles, text boxes, instructions, field and button labels, and other visual elements on the Portal Page Customization tab.

Character Limits for Portal Pages Titles, Content and Labels

The navigation paths for these portal page UI elements are:

- For Device portals, choose Administration > Device Portal Management > (any Portals) > Edit > Portal Page Customization > Pages.

Use this information when you enter content in the titles, text boxes, instructions, field and button labels, and other visual elements of the portal page the you are customizing. These updates are applied only to the specific page that you are customizing.

Note

Whether you enter single-byte or multi-byte characters, you can only enter the maximum number of characters identified for a field. Multi-byte characters do not affect the character limit.
<table>
<thead>
<tr>
<th>Field Category</th>
<th>Fields</th>
<th>Field Labels: Minimum Characters</th>
<th>Field Labels: Maximum Characters</th>
<th>Field Input Values: Minimum Characters</th>
<th>Field Input Values: Maximum Characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common page elements</td>
<td>Banner title</td>
<td></td>
<td>256</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Footer elements</td>
<td></td>
<td></td>
<td>0</td>
<td>2000</td>
</tr>
<tr>
<td></td>
<td>Browser Page Title</td>
<td></td>
<td></td>
<td>0</td>
<td>256</td>
</tr>
<tr>
<td></td>
<td>Instructional Text</td>
<td></td>
<td></td>
<td>0</td>
<td>2000</td>
</tr>
<tr>
<td></td>
<td>Content Title</td>
<td></td>
<td></td>
<td>0</td>
<td>256</td>
</tr>
<tr>
<td></td>
<td>Optional Content 1</td>
<td></td>
<td></td>
<td>0</td>
<td>2000</td>
</tr>
<tr>
<td></td>
<td>Optional Content 2</td>
<td></td>
<td></td>
<td>0</td>
<td>2000</td>
</tr>
<tr>
<td></td>
<td>Button labels</td>
<td>0</td>
<td>64</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check box labels</td>
<td>0</td>
<td>64</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tab labels</td>
<td>0</td>
<td>64</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Link labels</td>
<td>0</td>
<td>256</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>AUP</td>
<td>AUP Text</td>
<td>0</td>
<td></td>
<td>50,000</td>
</tr>
<tr>
<td></td>
<td>Message text</td>
<td>Message text (displayed on page)</td>
<td>0</td>
<td></td>
<td>2000</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Message text (displayed in pop-up window)</td>
<td>0</td>
<td></td>
<td>256</td>
</tr>
<tr>
<td></td>
<td>All fields labels</td>
<td>0</td>
<td>256</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Field input (general)</td>
<td>Field input in general (see special cases below)</td>
<td>0</td>
<td></td>
<td>256</td>
</tr>
<tr>
<td></td>
<td>Access Code field</td>
<td></td>
<td>1</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Registration Code field</td>
<td></td>
<td>1</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Username fields</td>
<td></td>
<td>1</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Password fields</td>
<td></td>
<td>1</td>
<td>256</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phone Number field</td>
<td></td>
<td>0</td>
<td>64</td>
<td></td>
</tr>
</tbody>
</table>
Portal Customization

You can customize the appearance of the end-user web portals and the guest experience. If you have experience with the cascading style sheet (CSS) language and with Javascript, you can use the jQuery Mobile ThemeRoller application to customize portal themes by changing the portal page layout.

You can view all the fields by exporting the CSS theme or language properties from the required portal page. Refer to the Export a Portal’s Default Theme CSS File for more information.

CSS Classes and Descriptions for End-User Portals Page Layout

Use these CSS classes to define and modify the page layout of the Cisco ISE end-user web portals.

<table>
<thead>
<tr>
<th>CSS Class Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cisco-ise-banner</td>
<td>Includes logos, banner image, and banner text.</td>
</tr>
<tr>
<td></td>
<td>On the Sponsor and My Devices portals, this class also contains buttons that</td>
</tr>
<tr>
<td></td>
<td>can activate a context menu. For example, the menu can bring up a pop-up</td>
</tr>
<tr>
<td></td>
<td>window with options to Log Out, Change Password, and so on.</td>
</tr>
<tr>
<td>cisco-ise-body</td>
<td>Contains all page elements that are not part of the banner.</td>
</tr>
<tr>
<td>cisco-ise-optional-content-1</td>
<td>Empty by default. You can add text, links, and HTML and Javascript code.</td>
</tr>
<tr>
<td>cisco-ise-main-content</td>
<td>Includes the main contents of the portal page, such as instructional text,</td>
</tr>
<tr>
<td></td>
<td>action buttons, and the cisco-ise-footer container.</td>
</tr>
<tr>
<td>cisco-ise-optional-content-2</td>
<td>Empty by default. You can add text, links, and HTML and Javascript code.</td>
</tr>
<tr>
<td>cisco-ise-footer</td>
<td>Part of the footer, it is a placeholder for links such as Contact Support</td>
</tr>
<tr>
<td></td>
<td>and online Help.</td>
</tr>
<tr>
<td>cisco-ise-footer-text</td>
<td>Empty by default. It is a placeholder for anything that you want to display</td>
</tr>
</tbody>
</table>
|                                        | at the bottom of the portal page, such as a copyright notice or a disclaimer.
HTML Support for a Portal Language File

The zipped language file for each portal includes the default language properties files for that portal. Each properties file includes dictionary keys that define the content that displays on the portal.

You can customize the text that displays on a portal, including the content in the Instructional Text, Content, Optional Content 1, and Optional Content 2 text boxes. Some of these text boxes have default content and some are empty.

Only some of these dictionary keys associated with these text boxes support HTML in their values (text).

HTML Support for the Blacklist Portal Language File

The navigation path to this portal's Instructional Text, Content, Optional Content 1, and Optional Content 2 text boxes is Administration > Device Portal Management > Blacklist Portal > Edit > Portal Page
**Customization > Pages.** You can use the View HTML Source icon in the mini-editor of the text boxes and add HTML code in your content.

These dictionary keys in the portal’s language properties files support HTML in their text.

---

**Note**

This is not a complete list of the dictionary keys in the files.

- key.blacklist.ui_reject_message

---

**HTML Support for Bring Your Own Device Portals Language Files**

The navigation path to this portal’s Instructional Text, Content, Optional Content 1, and Optional Content 2 text boxes is Administration > Device Portal Management > BYOD Portals > Edit > Portal Page Customization > Pages. You can use the View HTML Source icon in the mini-editor of the text boxes and add HTML code in your content.

These dictionary keys in the portal’s language properties files support HTML in their text.

---

**Note**

This is not a complete list of the dictionary keys in the files.

- key.guest.ui_contact_instruction_message
- key.guest.ui_byod_welcome_optional_content_1
- key.guest.ui_byod_welcome_optional_content_2
- key.guest.ui_byod_reg_limit_message
- key.guest.ui_byod_reg_content_message
- key.guest.ui_byod_success_manual_reconnect_message
- key.guest.ui_byod_install_winmac_instruction_message
- key.guest.ui_byod_install_optional_content_1
- key.guest.ui_byod_reg_optional_content_1
- key.guest.ui_byod_reg_optional_content_2
- key.guest.ui_byod_install_optional_content_2
- key.guest.ui_byod_reg_optional_content_2
- key.guest.ui_byod_reg_instruction_message
- key.guest.ui_byod_reg_instruction_message
- key.guest.ui_byod_welcome_aup_text
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_byod_install_ios_instruction_message
- key.guest.ui_byod_install_winxmac_instruction_message
- key.guest.ui_byod_welcome_instruction_message
HTML Support for Certificate Provisioning Portal Language Files

The navigation path to this portal's Instructional Text, Content, Optional Content 1, and Optional Content 2 text boxes is Administration > Device Portal Management > Certificate Provisioning Portal > Edit > Portal Page Customization > Pages. You can use the View HTML Source icon in the mini-editor of the text boxes and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

Note
This is not a complete list of the dictionary keys in the files.

- key.guest.ui_error_optional_content_2
- key.guest.ui_error_optional_content_1
- key.guest.ui_byod_welcome_renew_cert_message
- key.guest.ui_byod_install_android_instruction_message
- key.guest.ui_byod_install_instruction_message
- key.guest.ui_byod_welcome_config_device_message
- key.guest.ui_byod_success_message
- key.guest.ui_byod_success_unsupported_device_message
- key.guest.ui_byod_success_optional_content_1
- key.guest.ui_byod_success_optional_content_2
- key.guest.ui_error_instruction_message
- key.manualcertprov.ui_login_instruction_message
- key.manualcertprov.ui_aup_instruction_message
- key.manualcertprov.ui_changepwd_instruction_message
- key.manualcertprov.ui_post_access_instruction_message
- key.manualcertprov.ui_status_csv_invalid_instruction_message
- key.manualcertprov.ui_login_optional_content_1
- key.manualcertprov.ui_login_optional_content_2
- key.manualcertprov.ui_aup_optional_content_1
- key.manualcertprov.ui_aup_optional_content_2
- key.manualcertprov.ui_changepwd_optional_content_1
- key.manualcertprov.ui_changepwd_optional_content_2
- key.manualcertprov.ui_post_access_optional_content_1
HTML Support for Client Provisioning Portals Language Files

The navigation path to this portal's Instructional Text, Content, Optional Content 1, and Optional Content 2 text boxes is Administration > Device Portal Management > Client Provisioning Portals > Edit > Portal Page Customization > Pages. You can use the View HTML Source icon in the mini-editor of the text boxes and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

Note
This is not a complete list of the dictionary keys in the files.

- key.guest.ui_client_provision_agent_installed_instructions_without_java_message
- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_client_provision_unable_to_detect_message
- key.guest.ui_client_provision_instruction_message
- key.guest.ui_client_provision_agent_installation_message
- key.guest.ui_client_provision_posture_agent_check_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
- key.guest.ui_success_instruction_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_contact_optional_content_1
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_client_provision_posture_check_compliant_message
- key.guest.ui_client_provision_optional_content_2
- key.guest.ui_client_provision_optional_content_1
- key.guest.ui_error_optional_content_2
• key.guest.ui_error_optional_content_1
• key.guest.ui_client_provision_posture_check_non_compliant_message
• key.guest.ui_vlan_install_message
• key.guest.ui_success_optional_content_1
• key.guest.ui_success_optional_content_2
• key.guest.ui_client_provision_posture_agent_scan_message

HTML Support for Credential Guest Portals Language Files

The navigation path to this portal’s Instructional Text, Content, Optional Content 1, and Optional Content 2 text boxes is Work Centers > Guest Access > Portals & Components > Guest Portals > Edit > Portal Page Customization > Pages. You can use the View HTML Source icon in the mini-editor of the text boxes and add HTML code in your content.

These dictionary keys in the portal’s language properties files support HTML in their text.

Note
This is not a complete list of the dictionary keys in the files.

• key.guest.ui_contact_instruction_message
• key.guest.ui_login_optional_content_1
• key.guest.ui_login_optional_content_2
• key.guest.ui_client_provision_unable_to_detect_message
• key.guest.ui_client_provision_instruction_message
• key.guest.ui_device_reg_optional_content_2
• key.guest.ui_device_reg_optional_content_1
• key.guest.ui_byod_success_manual_reconnect_message
• key.guest.ui_byod_reg_optional_content_2
• key.guest.ui_byod_reg_optional_content_1
• key.guest.ui_client_provision_agent_installation_instructions_with_no_java_message
• key.guest.ui_success_instruction_message
• key.guest.ui_max_devices_instruction_message
• key.guest.ui_max_devices_optional_content_1
• key.guest.ui_self_reg_results_instruction_message
• key.guest.notification_credentials_email_body
• key.guest.ui_max_devices_optional_content_2
• key.guest.ui_post_access_message
• key.guest.ui_vlan_instruction_message
• key.guest.ui_byod_install_winmac_instruction_message
• key.guest.ui_aup_guest_text
• key.guest.ui_byod_install_optional_content_1
• key.guest.ui_byod_install_optional_content_2
• key.guest.ui_byod_reg_instruction_message
• key.guest.ui_aup_optional_content_1
• key.guest.ui_aup_optional_content_2
• key.guest.ui_self_reg_aup_text
• key.guest.ui_login_instruction_message
• key.guest.ui_vlan_optional_content_1
• key.guest.ui_vlan_optional_content_2
• key.guest.ui_self_reg_results_aup_text
• key.guest.ui_device_reg_register_message
• key.guest.ui_byod_welcome_instruction_message
• key.guest.ui_client_provision_optional_content_2
• key.guest.ui_self_reg_instruction_message
• key.guest.ui_vlan_install_message
• key.guest.ui_success_optional_content_1
• key.guest.ui_success_optional_content_2
• key.guest.ui_post_access_instruction_message
• key.guest.ui_post_access_optional_content_2
• key.guest.ui_post_access_optional_content_1
• key.guest.ui_byod_welcome_config_device_message
• key.guest.ui_client_provision_posture_agent_scan_message

**HTML Support for Hotspot Guest Portals Language Files**

The navigation path to this portal's Instructional Text, Content, Optional Content 1, and Optional Content 2 text boxes is Work Centers > Guest Access > Portals & Components > Guest Portals > Edit > Portal Page Customization > Pages. You can use the View HTML Source icon in the mini-editor of the text boxes and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.
This is not a complete list of the dictionary keys in the files.

- key.guest.ui_contact_instruction_message
- key.guest.ui_success_message
- key.guest.ui_post_access_message
- key.guest.ui_vlan_instruction_message
- key.guest.ui_success_instruction_message
- key.guest.ui_aup_optional_content_1
- key.guest.ui_aup_optional_content_2
- key.guest.ui_vlan_unsupported_error_message
- key.guest.ui_vlan_optional_content_1
- key.guest.ui_vlan_optional_content_2
- key.guest.ui_contact_optional_content_2
- key.guest.ui_contact_optional_content_1
- key.guest.ui_aup_instruction_message
- key.guest.ui_aup_hotspot_text
- key.guest.ui_vlan_execute_message
- key.guest.ui_vlan_install_message
- key.guest.ui_success_optional_content_1
- key.guest.ui_success_optional_content_2
- key.guest.ui_post_access_instruction_message
- key.guest.ui_post_access_optional_content_2
- key.guest.ui_post_access_optional_content_1

### HTML Support for Mobile Device Management Portals Language Files

The navigation path to this portal’s Instructional Text, Content, Optional Content 1, and Optional Content 2 text boxes is Administration > Device Portal Management > MDM Portals > Edit > Portal Page Customization > Pages. You can use the View HTML Source icon in the mini-editor of the text boxes and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

This is not a complete list of the dictionary keys in the files.
HTML Support for My Devices Portals Language Files

The navigation path to this portal's Instructional Text, Content, Optional Content 1, and Optional Content 2 text boxes is Administration > Device Portal Management > My Devices Portals > Edit > Portal Page Customization > Pages. You can use the View HTML Source icon in the mini-editor of the text boxes and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

Note

This is not a complete list of the dictionary keys in the files.
HTML Support for Sponsor Portals Language Files

The navigation path to this portal’s Instructional Text, Content, Optional Content 1, and Optional Content 2 text boxes is Work Centers > Guest Access > Portals & Components > Sponsor Portals > Edit > Portal Page Customization > Pages. You can use the View HTML Source icon in the mini-editor of the text boxes and add HTML code in your content.

These dictionary keys in the portal's language properties files support HTML in their text.

- key.mydevices.ui_home_instruction_message
- key.mydevices.ui_edit_optional_content_1
- key.mydevices.ui_edit_optional_content_2
- key.mydevices.ui_add_instruction_message
- key.mydevices.ui_post_access_optional_content_2
- key.mydevices.ui_post_access_optional_content_1
- key.mydevices.ui_error_instruction_message
- key.mydevices.ui_actions_instruction_message
- key.mydevices.ui_home_optional_content_2
- key.mydevices.ui_aup_optional_content_1
- key.mydevices.ui_aup_optional_content_2
- key.mydevices.ui_home_optional_content_1
- key.mydevices.ui_changepwd_instruction_message
- key.mydevices.ui_contact_instruction_message
- key.mydevices.ui_aup_employee_text
- key.mydevices.ui_login_optional_content_2
- key.mydevices.ui_login_optional_content_1
- key.mydevices.ui_login_instruction_message
- key.mydevices.ui_error_optional_content_1
- key.mydevices.ui_error_optional_content_2
- key.mydevices.ui_aup_instruction_message

Note

This is not a complete list of the dictionary keys in the files.

- key.sponsor.ui_aup_instruction_message
- key.sponsor.ui_create_random_instruction_message
Policy User Interface Reference

- Policy Set Settings, on page 1079
- Endpoint Profiling Policies Settings, on page 1085
- Endpoint Context Visibility Using UDID Attribute, on page 1090
- Dictionaries, on page 1090
- Special Conditions, on page 1091
- Results, on page 1116

Policy Set Settings

This section describes the Policy Set pages, which allow you to configure rule-based policy sets that include authentication, authorization and exception policies.

Policy Set Main Page—Configuration Settings

The following table describes the fields in the Policy Sets page, from which you can configure policy sets, including authentication, exception and authorization policies. For network access policies, choose Work Centers > Network Access > Policy Sets. For device administration policies, choose Work Centers > Device Administration > Device Admin Policy Sets.
### Table 130: Policy Set Configuration Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Choose the status of this policy. It can be one of the following: \n</td>
</tr>
<tr>
<td>Policy Set Name</td>
<td>Enter a unique name for this policy set.</td>
</tr>
<tr>
<td>Conditions</td>
<td>From a new policy row, click the plus (+) icon or from an existing policy row, click the Edit icon to open the Conditions Studio.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a unique description for the policy.</td>
</tr>
<tr>
<td>Allowed Protocols / Server Sequence</td>
<td>Choose an allowed protocol that you have already created, or click the (+) sign to Create a New Allowed Protocol, to Create a New Radius Sequence, or to Create a TACACS Sequence.</td>
</tr>
<tr>
<td>Conditions</td>
<td>From a new exceptions row, click the plus (+) icon or from an existing exception row, click the Edit icon to open the Conditions Studio.</td>
</tr>
<tr>
<td>Hits</td>
<td>Hits are a diagnostic tool indicating the number of times the conditions have matched. Hover over the icon to view when this was last updated, reset to zero and to view the frequency of updates.</td>
</tr>
</tbody>
</table>
## Authentication Policy Configuration Settings

The following table describes the fields in the Authentication Policy section of the Policy Sets Set view page, from which you can configure authentication sub-policies as part of your policy sets. For network access policies, choose **Work Centers > Network Access > Policy Sets**. For device administration policies, choose **Work Centers > Device Administration > Device Admin Policy Sets**. From the Policy Sets page, choose **View > Authentication Policy**.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>Click the cog icon from the Actions column to view and select different actions:</td>
</tr>
<tr>
<td></td>
<td>• Insert new row above—insert a new policy above the policy from which you opened the Actions menu.</td>
</tr>
<tr>
<td></td>
<td>• Insert new row below—insert a new policy below the policy from which you opened the Actions menu.</td>
</tr>
<tr>
<td></td>
<td>• Duplicate above—insert a duplicate policy above the policy from which you opened the Actions menu, above the original set.</td>
</tr>
<tr>
<td></td>
<td>• Duplicate below—insert a duplicate policy below the policy from which you opened the Actions menu, below the original set.</td>
</tr>
<tr>
<td></td>
<td>• Delete—delete the policy set.</td>
</tr>
<tr>
<td>View</td>
<td>Click the arrow icon to open the Set view of the specific policy set and view its authentication, exception and authorization sub-policies.</td>
</tr>
</tbody>
</table>
Table 131: Authentication Policy Configuration Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Choose the status of this policy. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Enabled—This policy condition is active.</td>
</tr>
<tr>
<td></td>
<td>• Disabled—This policy condition is inactive and will not be evaluated.</td>
</tr>
<tr>
<td></td>
<td>• Monitor Only—This policy condition will be evaluated, but the result will not be enforced. You can view the results of this policy condition</td>
</tr>
<tr>
<td></td>
<td>in the Live Log authentication page. In this, see the detailed report which will have the monitored step and attribute. For example, you may want</td>
</tr>
<tr>
<td></td>
<td>to add a new policy condition, but are not sure if the condition would provide you with the correct results. In this situation, you can create</td>
</tr>
<tr>
<td></td>
<td>the policy condition in monitored mode to view the results and then enable it if you are satisfied with the results.</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Enter a name for this authentication policy.</td>
</tr>
<tr>
<td>Conditions</td>
<td>From a new policy row, click the plus (+) icon or from an existing policy row, click the Edit icon to open the Conditions Studio.</td>
</tr>
<tr>
<td>Use</td>
<td>Choose the identity source that you want to use for authentication. You can also choose an identity source sequence if you have configured it.</td>
</tr>
<tr>
<td></td>
<td>You can edit the default identity source that you want Cisco ISE to use in case none of the identity sources defined in this rule match the request.</td>
</tr>
<tr>
<td>Options</td>
<td>Define a further course of action for authentication failure, user not found, or process failure events. You can choose one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• Reject—A reject response is sent.</td>
</tr>
<tr>
<td></td>
<td>• Drop—No response is sent.</td>
</tr>
<tr>
<td></td>
<td>• Continue—Cisco ISE proceeds with the authorization policy.</td>
</tr>
<tr>
<td>Hits</td>
<td>Hits are a diagnostic tool indicating the number of times the conditions have matched.</td>
</tr>
</tbody>
</table>
### Local and Global Exceptions Configuration Settings

For network access policies, choose Work Centers > Network Access > Policy Sets. For device administration policies, choose Work Centers > Device Administration > Device Admin Policy Sets. From the Policy Sets page, choose View > Local Exceptions Policy or Global Exceptions Policy.

Authorization exception settings are identical to the Authorization policy settings and are as described in Authorization Policy Settings, on page 1083.

### Authorization Policy Settings

The following table describes the fields in the Authorization Policy section of the Policy Sets Set view page, from which you can configure authorization policies as part of your policy sets. For network access policies, choose Work Centers > Network Access > Policy Sets. For device administration policies, choose Work Centers > Device Administration > Device Admin Policy Sets. From the Policy Sets page, choose View > Authorization Policy.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actions</td>
<td>Click the cog icon 🔄 from the Actions column to view and select different actions:</td>
</tr>
<tr>
<td></td>
<td>• Insert new row above—insert a new authentication policy above the policy from which you opened the Actions menu.</td>
</tr>
<tr>
<td></td>
<td>• Insert new row below—insert a new authentication policy below the policy from which you opened the Actions menu.</td>
</tr>
<tr>
<td></td>
<td>• Duplicate above—insert a duplicate authentication policy above the policy from which you opened the Actions menu, above the original set.</td>
</tr>
<tr>
<td></td>
<td>• Duplicate below—insert a duplicate authentication policy below the policy from which you opened the Actions menu, below the original set.</td>
</tr>
<tr>
<td></td>
<td>• Delete—delete the policy set.</td>
</tr>
</tbody>
</table>
**Table 132: Authorization Policy Configuration Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Choose the status of this policy. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Enabled—This policy condition is active.</td>
</tr>
<tr>
<td></td>
<td>• Disabled—This policy condition is inactive and will not be evaluated.</td>
</tr>
<tr>
<td></td>
<td>• Monitor Only—This policy condition will be evaluated, but the result will not be enforced. You can view the results of this policy condition in the Live Log authentication page.</td>
</tr>
<tr>
<td></td>
<td>In this, see the detailed report which will have the monitored step and attribute. For example, you may want to add a new policy condition, but are not sure if the condition would provide you with the correct results. In this situation, you can create the policy condition in monitored mode to view the results and then enable it if you are satisfied with the results.</td>
</tr>
<tr>
<td>Rule Name</td>
<td>Enter a unique name for this policy.</td>
</tr>
<tr>
<td>Conditions</td>
<td>From a new policy row, click the plus (+) icon or from an existing policy row, click the Edit icon to open the Conditions Studio.</td>
</tr>
<tr>
<td>Results/Profiles</td>
<td>Select the relevant authorization profile, which determines the different levels of permissions offered to the configured security group. If you have not yet configured the relevant authorization profile, you can do so inline.</td>
</tr>
<tr>
<td>Results/Security Groups</td>
<td>Select the relevant security group, which determines the groups of users relevant to the specific rule. If you have not yet configured the relevant security group, you can do so inline.</td>
</tr>
<tr>
<td>Results/Command Sets</td>
<td>Command sets enforce the specified list of commands that can be executed by a device administrator. When a device administrator issues operational commands on a network device, ISE is queried to determine whether the administrator is authorized to issue these commands. This is also referred to as command authorization.</td>
</tr>
<tr>
<td>Results/Shell Profiles</td>
<td>TACACS+ shell profiles control the initial login session of the device administrator.</td>
</tr>
</tbody>
</table>
### Endpoint Profiling Policies Settings

The following table describes the fields in the Endpoint Policies page. The navigation path for this page is: **Policy > Profiling > Profiling Policies**.

**Table 133: Endpoint Profiling Policies Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the endpoint profiling policy that you want to create.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description of the endpoint profiling policy that you want to create.</td>
</tr>
</tbody>
</table>
| Policy Enabled          | By default, the **Policy Enabled** check box is checked to associate a matching profiling policy when you profile an endpoint.  
                          | When unchecked, the endpoint profiling policy is excluded when you profile an endpoint. |
| Minimum Certainty Factor| Enter the minimum value that you want to associate with the profiling policy. The default value is 10. |
### Field Definitions and Usage Guidelines

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exception Action</td>
<td>Choose an exception action, which you want to associate with the conditions when defining a rule in the profiling policy.</td>
</tr>
<tr>
<td></td>
<td>The default is NONE. The exception actions are defined in the following location: Policy &gt; Policy Elements &gt; Results &gt; Profiling &gt; Exception Actions.</td>
</tr>
<tr>
<td>Network Scan (NMAP) Action</td>
<td>Choose a network scan action from the list, which you want to associate with the conditions when defining a rule in the profiling policy, if required.</td>
</tr>
<tr>
<td></td>
<td>The default is NONE. The exception actions are defined in the following location: Policy &gt; Policy Elements &gt; Results &gt; Profiling &gt; Network Scan (NMAP) Actions.</td>
</tr>
</tbody>
</table>
| Create an Identity Group for the policy | Check one of the following options to create an endpoint identity group:  
  • Yes, create matching Identity Group  
  • No, use existing Identity Group hierarchy |
| Yes, create matching Identity Group | Choose this option to use an existing profiling policy.  
  This option creates a matching identity group for those endpoints and the identity group will be the child of the Profiled endpoint identity group when an endpoint profile matches an existing profiling policy.  
  For example, the Xerox-Device endpoint identity group is created in the Endpoints Identity Groups page when endpoints discovered on your network match the Xerox-Device profile. |
### Fields

<table>
<thead>
<tr>
<th>No, use existing Identity Group hierarchy</th>
<th>Check this check box to assign endpoints to the matching parent endpoint identity group using hierarchical construction of profiling policies and identity groups. This option allows you to make use of the endpoint profiling policies hierarchy to assign endpoints to one of the matching parent endpoint identity groups, as well as to the associated endpoint identity groups to the parent identity group. For example, endpoints that match an existing profile are grouped under the appropriate parent endpoint identity group. Here, endpoints that match the Unknown profile are grouped under Unknown, and endpoints that match an existing profile are grouped under the Profiled endpoint identity group. For example, • If endpoints match the Cisco-IP-Phone profile, then they are grouped under the Cisco-IP-Phone endpoint identity group. • If endpoints match the Workstation profile, then they are grouped under the Workstation endpoint identity group. The Cisco-IP-Phone and Workstation endpoint identity groups are associated to the Profiled endpoint identity group in the system.</th>
</tr>
</thead>
</table>

### Parent Policy

Choose a parent profiling policy that are defined in the system to which you want to associate the new endpoint profiling policy. You can choose a parent profiling policy from which you can inherit rules and conditions to its child.

### Associated CoA Type

Choose one of the following CoA types that you want to associate with the endpoint profiling policy:

- No CoA
- Port Bounce
- Reauth
- Global Settings that is applied from the profiler configuration set in Administration > System > Settings > Profiling
### Fields

<table>
<thead>
<tr>
<th>Rules</th>
<th>Usage Guidelines</th>
</tr>
</thead>
</table>
| One or more rules that are defined in endpoint profiling policies determine the matching profiling policy for endpoints, which allows you to group endpoints according to their profiles.

One or more profiling conditions from the policy elements library are used in rules for validating endpoint attributes and their values for the overall classification. |

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Usage Guidelines</th>
</tr>
</thead>
</table>
| Click the plus [+] sign to expand the Conditions anchored overlay, and click the minus [-] sign, or click outside the anchored overlay to close it.

Click **Select Existing Condition from Library** or **Create New Condition (Advanced Option)**.

**Select Existing Condition from Library**---You can define an expression by selecting Cisco predefined conditions from the policy elements library.

**Create New Condition (Advanced Option)**---You can define an expression by selecting attributes from various system or user-defined dictionaries.

You can associate one of the following with the profiling conditions:

- An integer value for the certainty factor for each condition
- Either an exception action or a network scan action for that condition

Choose one of the following predefined settings to associate with the profiling condition:

- **Certainty Factor Increases**—Enter the certainty value for each rule, which can be added for all the matching rules with respect to the overall classification.
- **Take Exception Action**—Triggers an exception action that is configured in the Exception Action field for this endpoint profiling policy.
- **Take Network Scan Action**—Triggers a network scan action that is configured in the Network Scan (NMAP) Action field for this endpoint profiling policy. |
<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Existing Condition from Library</td>
<td>You can do the following:</td>
</tr>
<tr>
<td></td>
<td>• You can choose Cisco predefined conditions that are available in the policy elements library, and then use an AND or OR operator to add multiple conditions.</td>
</tr>
<tr>
<td></td>
<td>• Click the Action icon to do the following in the subsequent steps:</td>
</tr>
<tr>
<td></td>
<td>• Add Attribute/Value—You can add ad-hoc attribute/value pairs</td>
</tr>
<tr>
<td></td>
<td>• Add Condition from Library—You can add Cisco predefined conditions</td>
</tr>
<tr>
<td></td>
<td>• Duplicate—Create a copy of the selected condition</td>
</tr>
<tr>
<td></td>
<td>• Add Condition to Library—You can save ad-hoc attribute/value pairs that you create to the policy elements library</td>
</tr>
<tr>
<td></td>
<td>• Delete—Delete the selected condition.</td>
</tr>
</tbody>
</table>

| Create New Condition (Advance Option)      | You can do the following:                                                                                                                        |
|                                            | • You can add ad-hoc attribute/value pairs to your expression, and then use an AND or OR operator to add multiple conditions.                  |
|                                            | • Click the Action icon to do the following in the subsequent steps:                                                                            |
|                                            |   • Add Attribute/Value—You can add ad-hoc attribute/value pairs                                                                               |
|                                            |   • Add Condition from Library—You can add Cisco predefined conditions                                                                       |
|                                            |   • Duplicate—Create a copy of the selected condition                                                                                         |
|                                            |   • Add Condition to Library—You can save ad-hoc attribute/value pairs that you create to the policy elements library                             |
|                                            |   • Delete—Delete the selected condition. Here, you can use the AND or OR operator                                                              |

Related Topics
- Cisco ISE Profiling Service, on page 643
- Create Endpoint Profiling Policies, on page 681
Endpoint Context Visibility Using UDID Attribute

The Unique Identifier (UDID) is an endpoint attribute used to identify MAC addresses that belong to an endpoint. An endpoint may contain multiple MAC addresses (for example, one MAC address for the wired interface and another for the wireless interface), and when AnyConnect is installed on an endpoint, the AnyConnect agent generates a UDID for the endpoint. The UDID is saved as an endpoint attribute and an endpoint can be queried using the UDID. The UDID remains constant for an endpoint and does not change with the AnyConnect installation or uninstallation. This facilitates the Context Visibility page (Context Visibility > Endpoints > Compliance) to display one entry instead of multiple entries for endpoints with multiple NICs. You can ensure posture control on a specific endpoint rather than on a Mac address.

Dictionaries

This section describes RADIUS vendor dictionaries used in Cisco ISE.

The following table describes the fields in the Dictionary page for RADIUS vendors, which allows you to configure dictionary attributes for the RADIUS vendors. The navigation path for this page is: Policy > Policy Elements > Dictionaries > System > RADIUS > RADIUS Vendors.

Table 134: RADIUS Vendor Dictionary Attribute Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Name</td>
<td>Enter the vendor specific attribute name for the selected RADIUS vendor.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter an optional description for the vendor specific attribute.</td>
</tr>
<tr>
<td>Internal Name</td>
<td>Enter the name for the vendor specific attribute that refers to it internally in the database.</td>
</tr>
<tr>
<td>Data Type</td>
<td>Choose one of the following data types for the vendor specific attribute:</td>
</tr>
<tr>
<td></td>
<td>• STRING</td>
</tr>
<tr>
<td></td>
<td>• OCTET_STRING</td>
</tr>
<tr>
<td></td>
<td>• UNIT32</td>
</tr>
<tr>
<td></td>
<td>• UNIT64</td>
</tr>
<tr>
<td></td>
<td>• IPV4</td>
</tr>
<tr>
<td></td>
<td>• IPV6</td>
</tr>
<tr>
<td><strong>Fields</strong></td>
<td><strong>Usage Guidelines</strong></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable MAC option</td>
<td>Check this check box to enable the comparison of RADIUS attribute as MAC address. By default, for the RADIUS attribute calling-station-id this option is marked as enabled and you cannot disable it. For other dictionary attributes (of string types) within the RADIUS vendor dictionary, you can enable or disable this option.</td>
</tr>
<tr>
<td></td>
<td>Once you enable this option, while setting the authentication and authorization conditions, you can define whether the comparison is clear string by selecting the Text option or whether it is MAC address by selecting the MAC address option.</td>
</tr>
<tr>
<td>Direction</td>
<td>Choose one of the options that applies to RADIUS messages:</td>
</tr>
<tr>
<td>ID</td>
<td>Enter the vendor attribute ID. The valid range is 0 to 255.</td>
</tr>
<tr>
<td>Allow Tagging</td>
<td>Check this check box to mark the attribute as being permitted to have a tag, as defined in RFC2868. The purpose of the tag is to allow grouping of attributes for tunnelled users. See RFC2868 for more details. The tagged attributes support ensures that all attributes pertaining to a given tunnel contain the same value in their respective tag fields, and that each set includes an appropriately-valued instance of the Tunnel-Preference attribute. This conforms to the tunnel attributes that are to be used in a multi-vendor network environment, thereby eliminating interoperability issues among Network Access Servers (NASs) manufactured by different vendors.</td>
</tr>
<tr>
<td>Allow multiple instances of this attribute in a profile</td>
<td>Check this check box when you want multiple instances of this RADIUS vendor specific attribute in profiles.</td>
</tr>
</tbody>
</table>

**Related Topics**

- System Defined Dictionaries and Dictionary Attributes, on page 261
- User-Defined Dictionaries and Dictionary Attributes, on page 262
- RADIUS-Vendor Dictionaries, on page 263
- Create RADIUS-Vendor Dictionaries, on page 264

**Special Conditions**

This section describes policy conditions used for profiling endpoints, posture clients, and to limit or extend permission to access to Cisco ISE system resources.
Profiler Condition Settings

The following table describes the fields in the Profiler Condition page. The navigation path for this page is: Policy > Policy Elements > Conditions > Profiling.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the profiler condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the profiler condition.</td>
</tr>
<tr>
<td>Type</td>
<td>Choose any one of the predefined types.</td>
</tr>
<tr>
<td>Attribute Name</td>
<td>Choose an attribute on which to base the profiler condition.</td>
</tr>
<tr>
<td>Operator</td>
<td>Choose an operator.</td>
</tr>
<tr>
<td>Attribute Value</td>
<td>Enter the value for the attribute that you have chosen. For Attribute Names that</td>
</tr>
<tr>
<td></td>
<td>contain pre-defined Attribute Values, this option displays a drop-down list with</td>
</tr>
<tr>
<td></td>
<td>the pre-defined values, and you can choose a value.</td>
</tr>
<tr>
<td>System Type</td>
<td>Profiling conditions can be any one of the following types:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Provided—Profiling conditions that are provided by Cisco ISE when</td>
</tr>
<tr>
<td></td>
<td>deployed are identified as Cisco Provided. You cannot edit or delete them from</td>
</tr>
<tr>
<td></td>
<td>the system.</td>
</tr>
<tr>
<td></td>
<td>• Administrator Created—Profiling conditions that you create as an administrator</td>
</tr>
<tr>
<td></td>
<td>of Cisco ISE are identified as Administrator Created.</td>
</tr>
</tbody>
</table>

Related Topics
- Cisco ISE Profiling Service, on page 643
- Profiler Conditions, on page 560
- Profiler Feed Service, on page 716
- Create a Profiler Condition, on page 560

Posture Condition Settings

This section describes simple and compound conditions used for posture.

File Condition Settings

The following table describes the fields in the File Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > File Condition.
# Table 136: File Condition Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines for Windows OS</th>
<th>Usage Guidelines for Mac OSX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the file condition.</td>
<td>Enter the name of the file condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the file condition.</td>
<td>Enter a description for the file condition.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Select any Windows operating system to which the file condition should be applied.</td>
<td>Select any Mac OSX to which the file condition should be applied.</td>
</tr>
<tr>
<td>File Type</td>
<td>Choose one of the predefined settings:</td>
<td>Choose one of the predefined settings:</td>
</tr>
<tr>
<td></td>
<td>• <strong>FileDate</strong>—Checks whether a file with a particular file-created or file-modified date exists on the system.</td>
<td>• <strong>FileDate</strong>—Checks whether a file with a particular file-created or file-modified date exists on the system.</td>
</tr>
<tr>
<td></td>
<td>• <strong>FileExistence</strong>—Checks whether a file exists on the system.</td>
<td>• <strong>FileExistence</strong>—Checks whether a file exists on the system.</td>
</tr>
<tr>
<td></td>
<td>• <strong>FileVersion</strong>—Checks whether a particular version of a file exists on the system.</td>
<td>• <strong>FileVersion</strong>—Checks whether a particular version of a file exists on the system.</td>
</tr>
<tr>
<td></td>
<td>• <strong>CRC32</strong>—Checks the data integrity of a file using the checksum function.</td>
<td>• <strong>CRC32</strong>—Checks the data integrity of a file using the checksum function.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SHA-256</strong>—Checks the data integrity of a file using the hash function.</td>
<td>• <strong>SHA-256</strong>—Checks the data integrity of a file using the hash function.</td>
</tr>
<tr>
<td></td>
<td>• <strong>PropertyList</strong>—Checks the property value in a plist file, such as loginwindow.plist.</td>
<td>• <strong>PropertyList</strong>—Checks the property value in a plist file, such as loginwindow.plist.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines for Windows OS</td>
<td>Usage Guidelines for Mac OSX</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>Data Type &amp; Operator</td>
<td>NA</td>
<td>(Available only if you select PropertyList as the File Type) Choose the data type or value of the key to be searched in the plist files. Each data type contains a set of operators.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Unspecified</strong>—Checks the existence of the specified key. Enter an Operator (Exists, DoesNotExist).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Number</strong>—Checks for the specified key of number data type. Enter an Operator (equals, does not equal, greater than, less than, greater than or equal to, less than or equal to) and a Value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>String</strong>—Checks for the specified key of string data type. Enter an Operator (equals, does not equal, equals (ignore case), starts with, does not start with, contains, does not contain, ends with, does not end with) and a Value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <strong>Version</strong>—Checks for the value of the specified key as a version string. Enter an Operator (earlier than, later than, same as) and a Value.</td>
</tr>
<tr>
<td>Property Name</td>
<td>NA</td>
<td>(Available only if you select PropertyList as the File Type) Enter a name of the key, for example, BuildVersionStampAsNumber</td>
</tr>
</tbody>
</table>
### Usage Guidelines for Windows OS

**File Path**

Choose one of the predefined settings:

- **ABSOLUTE_PATH**—Checks the file in the fully qualified path of the file. For example, `C:\<directory>\filename`. For other settings, enter only the file name.

- **SYSTEM_32**—Checks the file in the `C:\WINDOWS\system32` directory. Enter the file name.

- **SYSTEM_DRIVE**—Checks the file in the `C:\` drive. Enter the file name.

- **SYSTEM_PROGRAMS**—Checks the file in the `C:\Program Files` directory. Enter the file name.

- **SYSTEM_ROOT**—Checks the file in the root path for Windows system. Enter the file name.

- **USER_DESKTOP**—Checks if the specified file is present on the Windows user's desktop. Enter the file name.

- **USER_PROFILE**—Checks if the file is present in the Windows user's local profile directory. Enter the file path.

**File Date Type**

(Available only if you select **FileDate** as the File Type) Choose **Creation Date** or **Modification Date**.

### Usage Guidelines for Mac OSX

Choose one of the predefined settings:

- **Root**—Checks the file in the root (`/`) directory. Enter the file path.

- **Home**—Checks the file in the home (`~`) directory. Enter the file path.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines for Windows OS</th>
<th>Usage Guidelines for Mac OSX</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Path</td>
<td>Choose one of the predefined settings:</td>
<td>Choose one of the predefined settings:</td>
</tr>
<tr>
<td></td>
<td>• <strong>ABSOLUTE_PATH</strong>—Checks the file in the fully qualified path of the file. For example, <code>C:\&lt;directory&gt;\filename</code>. For other settings, enter only the file name.</td>
<td>• <strong>Root</strong>—Checks the file in the root (<code>/</code>) directory. Enter the file path.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SYSTEM_32</strong>—Checks the file in the <code>C:\WINDOWS\system32</code> directory. Enter the file name.</td>
<td>• <strong>Home</strong>—Checks the file in the home (<code>~</code>) directory. Enter the file path.</td>
</tr>
<tr>
<td></td>
<td>• <strong>SYSTEM_DRIVE</strong>—Checks the file in the <code>C:\</code> drive. Enter the file name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SYSTEM_PROGRAMS</strong>—Checks the file in the <code>C:\Program Files</code> directory. Enter the file name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>SYSTEM_ROOT</strong>—Checks the file in the root path for Windows system. Enter the file name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>USER_DESKTOP</strong>—Checks if the specified file is present on the Windows user's desktop. Enter the file name.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• <strong>USER_PROFILE</strong>—Checks if the file is present in the Windows user's local profile directory. Enter the file path.</td>
<td></td>
</tr>
<tr>
<td>File Date Type</td>
<td>(Available only if you select <strong>FileDate</strong> as the File Type) Choose <strong>Creation Date</strong> or <strong>Modification Date</strong>.</td>
<td>(Available only if you select <strong>FileDate</strong> as the File Type) Choose <strong>Creation Date</strong> or <strong>Modification Date</strong>.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines for Windows OS</td>
<td>Usage Guidelines for Mac OSX</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>File Operator/Operator</td>
<td>The File Operator options change according to the settings you select in the File Type. Choose the settings appropriately:</td>
<td>The File Operator options change according to the settings you select in the File Type. Choose the settings appropriately:</td>
</tr>
<tr>
<td>FileDate</td>
<td>• EarlierThan&lt;br&gt;• LaterThan&lt;br&gt;• EqualTo</td>
<td>FileDate&lt;br&gt;• EarlierThan&lt;br&gt;• LaterThan&lt;br&gt;• EqualTo</td>
</tr>
<tr>
<td>FileExistence</td>
<td>• Exists&lt;br&gt;• DoesNotExist</td>
<td>FileExistence&lt;br&gt;• Exists&lt;br&gt;• DoesNotExist</td>
</tr>
<tr>
<td>FileVersion</td>
<td>• EarlierThan&lt;br&gt;• LaterThan&lt;br&gt;• EqualTo</td>
<td></td>
</tr>
<tr>
<td>File CRC Data</td>
<td>(Available only if you select <strong>CRC32</strong> as the File Type) You can enter a checksum value, for example, 0x3c37fec3 to check file integrity. The checksum value should start with 0x, a hexadecimal integer.</td>
<td>(Available only if you select <strong>CRC32</strong> as the File Type) You can enter a checksum value, for example, 0x3c37fec3 to check file integrity. The checksum value should start with 0x, a hexadecimal integer.</td>
</tr>
<tr>
<td>File SHA-256 Data</td>
<td>(Available only if you select <strong>SHA-256</strong> as the File Type) You can enter a 64-byte hexadecimal hash value to check file integrity.</td>
<td>(Available only if you select <strong>SHA-256</strong> as the File Type) You can enter a 64-byte hexadecimal hash value to check file integrity.</td>
</tr>
<tr>
<td>Date and Time</td>
<td>(Available only if you select <strong>FileDate</strong> as the File Type) Enter the date and time of the client system in mm/dd/yyyy and hh:mm:ss format.</td>
<td>(Available only if you select <strong>FileDate</strong> as the File Type) Enter the date and time of the client system in mm/dd/yyyy and hh:mm:ss format.</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Simple Posture Conditions](#), on page 561
- [Compound Posture Conditions](#), on page 562
- [Create a Posture Condition](#), on page 801
Firewall Condition Settings

The Firewall condition checks if a specific Firewall product is running on an endpoint. The list of supported Firewall products is based on the OPSWAT support charts. You can enforce policies during initial posture and Periodic Reassessment (PRA).

Cisco ISE provides default Firewall conditions for Windows and Mac OS. These conditions are disabled by default.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the Firewall condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the Firewall condition.</td>
</tr>
<tr>
<td>Compliance Module</td>
<td>Choose the required compliance module.</td>
</tr>
<tr>
<td></td>
<td>• 4.x or later</td>
</tr>
<tr>
<td></td>
<td>• 3.x or later</td>
</tr>
<tr>
<td></td>
<td>• Any Version</td>
</tr>
<tr>
<td>Operating System</td>
<td>Checks If the required Firewall product is installed on an endpoint. You can select the Windows OS or Mac OSX.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Choose a vendor name from the drop-down list. The Firewall products of a vendor and their check type are retrieved and displayed in the Products for Selected Vendor table. The list in the table changes according to the selected operating system.</td>
</tr>
<tr>
<td>Check Type</td>
<td>Enabled: To check if a specific Firewall is running on an endpoint. Verify if the vendor's product supports the chosen check type by referring to the Products for Selected Vendor list.</td>
</tr>
</tbody>
</table>

Registry Condition Settings

The following table describes the fields in the Registry Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Registry Condition.

Table 137: Registry Condition Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the registry condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the registry condition.</td>
</tr>
<tr>
<td>Registry Type</td>
<td>Choose one of the predefined settings as the registry type.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Registry Root Key</td>
<td>Choose one of the predefined settings as the registry root key.</td>
</tr>
<tr>
<td>Sub Key</td>
<td>Enter the sub key without the backslash (&quot;) to check the registry key in the path specified in the Registry Root Key. For example, SOFTWARE\Symantec\Norton AntiVirus\version will check the key in the following path: HKLM\SOFTWARE\Symantec\NortonAntiVirus\version</td>
</tr>
<tr>
<td>Value Name</td>
<td>(Available only if you select RegistryValue or RegistryValueDefault as the Registry Type) Enter the name of the registry key value to be checked for RegistryValue. This is the default field for RegistryValueDefault.</td>
</tr>
<tr>
<td>Value Data Type</td>
<td>(Available only if you select RegistryValue or RegistryValueDefault as the Registry Type) Choose one of the following settings:</td>
</tr>
<tr>
<td></td>
<td>• Unspecified—Checks whether the registry key value exists or not. This option is available only for RegistryValue.</td>
</tr>
<tr>
<td></td>
<td>• Number—Checks the specified number in the registry key value</td>
</tr>
<tr>
<td></td>
<td>• String—Checks the string in the registry key value</td>
</tr>
<tr>
<td></td>
<td>• Version—Checks the version in the registry key value</td>
</tr>
<tr>
<td>Value Operator</td>
<td>Choose the settings appropriately.</td>
</tr>
<tr>
<td>Value Data</td>
<td>(Available only if you select RegistryValue or RegistryValueDefault as the Registry Type) Enter the value of the registry key according to the data type you have selected in Value Data Type.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Select the operating system to which the registry condition should be applied.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Simple Posture Conditions, on page 561
- Compound Posture Conditions, on page 562
Application Condition Settings

The following table describes the fields in the Application Conditions page. The navigation path for this page is: **Policy > Policy Elements > Conditions > Posture > Application Condition**.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the application condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the application condition.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Select the Windows OS or the MAC OSX to which the application condition should be applied.</td>
</tr>
<tr>
<td>Process Name</td>
<td>Enter the name of the application to be checked.</td>
</tr>
<tr>
<td>Application Operator</td>
<td>Choose the status to be checked.</td>
</tr>
</tbody>
</table>

Related Topics

- Simple Posture Conditions, on page 561
- Compound Posture Conditions, on page 562

Continuous Endpoint Attribute Monitoring

You can use the AnyConnect agent to continuously monitor different endpoint attributes to ensure that dynamic changes are observed during posture assessment. This improves the overall visibility of an endpoint and helps you create posture policies based on their behavior. The AnyConnect agent monitors applications that are installed and running on an endpoint. You can turn on and off the feature and configure how often the data should be monitored. By default, data is collected every 5 minutes and is stored in the database. During initial posture, AnyConnect reports a complete list of running and installed applications. After initial posture, the AnyConnect agent scans the applications every X minute and sends the differences from the last scan to the server. The server displays the complete list of running and installed applications.

Application Condition Settings

The application condition queries for applications that are installed on an endpoint. This helps you get an aggregate visibility of the software distributed on your endpoints. For example, based on the information, you can create policies and work with the Desktop team to reduce software licenses.

The following list describes the fields in the Application Conditions page. The navigation path to this page is: **Work Centers > Posture > Policy Elements > Application Condition > Add**.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the application condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description for the application condition.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Select the Windows OS or MAC OSX to which the application condition should be applied.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Compliance Module</td>
<td>Support for OESIS version 4.x or later, 3.x or earlier, or Any Version.</td>
</tr>
<tr>
<td>Check By</td>
<td>Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Process</strong>—Check the option to check if a process is running on an endpoint.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Application</strong>—Check the option to check if an application is running on an endpoint.</td>
</tr>
<tr>
<td>Process Name</td>
<td>(Available when you select <strong>Process</strong> as the Check By option) Enter the required process name.</td>
</tr>
<tr>
<td>Application Operator</td>
<td>(Available when you select <strong>Process</strong> as the Check By option) Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Running</strong>—Select the option to check if an application is running on an endpoint.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Not Running</strong>—Select the option to check if an application is not running on an endpoint.</td>
</tr>
<tr>
<td>Application State</td>
<td>(Available when you select <strong>Application</strong> as the Check By option) Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Installed</strong>—Check the option to find if clients have malicious applications installed in their systems. If a malicious application is found, the remediation action is triggered.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Running</strong>—Check the option to check if an application is running on an endpoint.</td>
</tr>
<tr>
<td>Provision By</td>
<td>(Available when you select <strong>Application</strong> as the Check By option) Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Everything</strong>—You can select all listed categories such as Browser, Patch Management, and so on.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Name</strong>—You should select at least one category. For example, if you choose the <strong>Browser</strong> category, it displays the corresponding vendors in the <strong>Vendor</strong> drop-down list.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Category</strong>—You can check one or more categories such as Anti-Malware, Backup, Browser, or Data Storage.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Categories are dynamically updated from the OPSWAT library.</td>
</tr>
</tbody>
</table>
You can view the number of installed and running applications for each endpoint in the **Context Visibility > Endpoints > Compliance** page.

The **Home > Summary > Compliance** page displays the percentage of endpoints that are subject to posture assessment and are compliant.

## Service Condition Settings

The following table describes the fields in the Service Conditions page. The navigation path for this page is: **Policy > Policy Elements > Conditions > Posture > Service Condition**.

### Table 139: Service Conditions Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the service condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the service condition.</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>Select the operating system to which the service condition should be applied. You can select different versions of the Windows OS or Mac OSX.</td>
</tr>
<tr>
<td>Service Name</td>
<td>Enter the name of the Daemon or User Agent service, for example, com.apple.geod, running as root. The AnyConnect agent uses the command <code>sudo launchctl list</code> to validate the service condition.</td>
</tr>
<tr>
<td>Service Type</td>
<td>Choose the type of service that AnyConnect should check for to ensure client compliance:</td>
</tr>
<tr>
<td></td>
<td>• Daemon—Checks if a specified service, such as scanning a client device for malware, is present in the specified list of Daemon services in the client.</td>
</tr>
<tr>
<td></td>
<td>• User Agent—Checks if a specified service, such as a service that runs when malware is detected, is present in the specified list of User services in the client.</td>
</tr>
<tr>
<td></td>
<td>• Daemon or User Agent—Checks if the specified services are present either in the Daemon or User Agent services list.</td>
</tr>
<tr>
<td>Service Operator</td>
<td>Choose the service status that you want to check in the client:</td>
</tr>
<tr>
<td></td>
<td>• Windows OS—To check if a service is <strong>Running</strong> or <strong>Not Running</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Mac OSX—To check if a service is <strong>Loaded</strong>, <strong>Not Loaded</strong>, <strong>Loaded &amp; Running</strong>, <strong>Loaded with Exit Code</strong>, and <strong>Loaded &amp; running or with Exit code</strong>.</td>
</tr>
</tbody>
</table>
**Posture Compound Condition Settings**

The following table describes the fields in the Compound Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Compound Condition.

<table>
<thead>
<tr>
<th><strong>Fields</strong></th>
<th><strong>Usage Guidelines</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the compound condition that you want to create.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description of the compound condition that you want to create.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Select one or more Windows operating systems. This allow you to associate Windows operating systems to which the condition is applied.</td>
</tr>
<tr>
<td>Parentheses ( )</td>
<td>Click the parentheses to combine two simple conditions from the following simple condition types: file, registry, application, and service conditions.</td>
</tr>
<tr>
<td>( &amp; )—AND operator (use “&amp;” for an AND operator, without the quotes)</td>
<td>You can use the AND operator (ampersand [ &amp; ]) in a compound condition. For example, enter <code>Condition1 &amp; Condition2</code>.</td>
</tr>
<tr>
<td>(</td>
<td>)—OR operator (use “</td>
</tr>
<tr>
<td>( ! )—NOT operator (use “!” for a NOT operator, without the quotes)</td>
<td>You can use the NOT operator (exclamation point [ ! ]) in a compound conditions. For example, enter <code>Condition1 &amp; Condition2</code>.</td>
</tr>
<tr>
<td>Simple Conditions</td>
<td>Choose from a list of simple conditions of the following types: file, registry, application, and service conditions. You can also create simple conditions of file, registry, application and service conditions from the object selector. Click the quick picker (down arrow) on the Action button to create simple conditions of file, registry, application, and service conditions.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Simple Posture Conditions, on page 561
- Compound Posture Conditions, on page 562
**AntiVirus Condition Settings**

The following table describes the fields in the Anti-Virus Condition page. The navigation path for this page is: **Policy > Policy Elements > Conditions > Posture > Anti-Virus Condition**.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the antivirus condition that you want to create.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description of the antivirus condition that you want to create.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Select an operating system to check the installation of an antivirus program on your client, or check the latest antivirus definition file updates to which the condition is applied.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Choose a vendor from the drop-down list. The selection of Vendor retrieves their antivirus products and versions, which are displayed in the Products for Selected Vendor table.</td>
</tr>
<tr>
<td>Check Type</td>
<td>Choose whether to check an installation or check the latest definition file update on the client.</td>
</tr>
<tr>
<td>Installation</td>
<td>Choose to check only the installation of an antivirus program on the client.</td>
</tr>
<tr>
<td>Definition</td>
<td>Choose to check only the latest definition file update of an antivirus product on the client.</td>
</tr>
<tr>
<td>Check against latest AV definition file version, if available. (Otherwise check against latest definition file date).</td>
<td>(Available only when you choose Definition check type) Choose to check the antivirus definition file version on the client against the latest antivirus definition file version, if available as a result of posture updates in Cisco ISE. Otherwise, this option allows you to check the definition file date on the client against the latest definition file date in Cisco ISE.</td>
</tr>
</tbody>
</table>
### AntiVirus Condition Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow virus definition file to be (Enabled)</td>
<td>(Available only when you choose Definition check type) Choose to check the antivirus definition file version and the latest antivirus definition file date on the client. The latest definition file date cannot be older than that you define in the next field (days older than field) from the latest antivirus definition file date of the product or the current system date. If unchecked, Cisco ISE allows you to check only the version of the antivirus definition file using the Check against latest AV definition file version, if available option.</td>
</tr>
<tr>
<td>days older than</td>
<td>Define the number of days that the latest antivirus definition file date on the client can be older from the latest antivirus definition file date of the product or the current system date. The default value is zero (0).</td>
</tr>
<tr>
<td>latest file date</td>
<td>Choose to check the antivirus definition file date on the client, which can be older by the number of days that you define in the days older than field. If you set the number of days to the default value (0), then the antivirus definition file date on the client should not be older than the latest antivirus definition file date of the product.</td>
</tr>
<tr>
<td>current system date</td>
<td>Choose to check the antivirus definition file date on the client, which can be older by the number of days that you define in the days older than field. If you set the number of days to the default value (0), then the antivirus definition file date on the client should not be older than the current system date.</td>
</tr>
<tr>
<td>Products for Selected Vendor</td>
<td>Choose an antivirus product from the table. Based on the vendor that you select in the New Anti-virus Condition page, the table retrieves information on their antivirus products and their version, remediation support that they provide, latest definition file date and its version. The selection of a product from the table allows you to check for the installation of an antivirus program, or check for the latest antivirus definition file date, and its latest version.</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Compound Posture Conditions](#), on page 562
- [Preconfigured Antivirus and Antispyware Conditions](#), on page 562
- [Antivirus and Antispyware Support Chart](#), on page 563
Antispyware Compound Condition Settings

The following table describes the fields in the AS Compound Conditions page. The navigation path for this page is: **Policy > Policy Elements > Conditions > AS Compound Condition**.

**Table 142: Antispyware Compound Condition Settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the antispyware compound condition that you want to create.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description of the antispyware compound condition that you want to create.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Selecting an operating system allows you to check the installation of an antispyware programs on your client, or check the latest antispyware definition file updates to which the condition is applied.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Choose a vendor from the drop-down list. The selection of Vendor retrieves their antispyware products and versions, which are displayed in the Products for Selected Vendor table.</td>
</tr>
<tr>
<td>Check Type</td>
<td>Choose if you want to choose a type whether to check an installation, or check the latest definition file update on the client.</td>
</tr>
<tr>
<td>Installation</td>
<td>Choose if you want to check only the installation of an antispyware program on the client.</td>
</tr>
<tr>
<td>Definition</td>
<td>Choose if you want to check only the latest definition file update of an antispyware product on the client.</td>
</tr>
<tr>
<td>Allow virus definition file to be (Enabled)</td>
<td>Check this check box when you are creating antispyware definition check types, and disabled when creating antispyware installation check types. If checked, the selection allows you to check antispyware definition file version and the latest antispyware definition file date on the client. The latest definition file date cannot be older than that you define in the days older than field from the current system date. If unchecked, the selection allows you to check only the version of the antispyware definition file as the Allow virus definition file to be check box is not checked.</td>
</tr>
<tr>
<td>days older than</td>
<td>Define the number of days that the latest antispyware definition file date on the client can be older from the current system date. The default value is zero (0).</td>
</tr>
</tbody>
</table>
### Usage Guidelines

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>The current system date</td>
<td>Choose to check the antispyware definition file date on the client, which can be older by the number of days that you define in the days older than field. If you set the number of days to the default value (0), then the antispyware definition file date on the client should not be older than the current system date.</td>
</tr>
<tr>
<td>Products for Selected Vendor</td>
<td>Choose an antispyware product from the table. Based on the vendor that you select in the New Anti-spyware Compound Condition page, the table retrieves information on their antispyware products and their version, remediation support that they provide, latest definition file date and its version. The selection of a product from the table allows you to check for the installation of an antispyware program, or check for the latest antispyware definition file date, and its latest version.</td>
</tr>
</tbody>
</table>

### Related Topics

- Compound Posture Conditions, on page 562
- Preconfigured Antivirus and Antispyware Conditions, on page 562
- Antivirus and Antispyware Support Chart, on page 563

### Antimalware Condition Settings

The antimalware condition is a combination of the antispyware and antivirus conditions and is supported by OESIS version 4.x or later compliance module. The following table describes the fields in the Antimalware Conditions page. The navigation path is: Work Centers > Posture > Posture Elements > Conditions > Antimalware. You can also access the option in the Policy > Policy Elements > Conditions > Posture > Antimalware Condition page.

### Note

It is recommended that you manually update the installed Antimalware products to have the latest definitions at least once. Otherwise, the posture checks using AnyConnect for Antimalware definitions will fail.

### Table 143: Antimalware Condition Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the antimalware condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the antimalware condition.</td>
</tr>
<tr>
<td>Compliance Module</td>
<td>Support for OESIS version 4.x or later.</td>
</tr>
<tr>
<td><strong>Field</strong></td>
<td><strong>Usage Guidelines</strong></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Operating System</td>
<td>Select an operating system to check the installation of antimalware programs on your client, or check the latest antimalware definition file updates to which the condition is applied. It supports both MAC and Windows OS.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Choose a vendor from the drop-down list. The selected vendor’s antimalware products, versions, latest definition dates, latest definition versions, and the minimum compliance module versions, are displayed in the Products for Selected Vendor table.</td>
</tr>
<tr>
<td>Check Type</td>
<td>Choose whether to check an installation or check the latest definition file update on the client.</td>
</tr>
<tr>
<td>Installation</td>
<td>Choose to check only the installation of an antimalware program on the client.</td>
</tr>
<tr>
<td>Definition</td>
<td>Choose to check only the latest definition file update of an antimalware product on the client.</td>
</tr>
<tr>
<td>Check against latest AV definition file version, if available. (Otherwise check against latest definition file date).</td>
<td>(Available only when you choose Definition check type) Choose to check the antimalware definition file version on the client against the latest antimalware definition file version, if available as a result of posture updates in Cisco ISE. Otherwise, this option allows you to check the definition file date on the client against the latest definition file date in Cisco ISE. This check will only work if there is a value listed in Cisco ISE for the Latest Definition Date or Latest Definition Version field for the selected product. Otherwise, the Current System Date field must be used.</td>
</tr>
<tr>
<td>Allow Virus Definition File to be (Enabled)</td>
<td>(Available only when you choose Definition check type) Choose to check the antimalware definition file version and the latest antimalware definition file date on the client. The latest definition file date cannot be older than that you define in the next field (days older than field) from the latest antimalware definition file date of the product or the current system date. If unchecked, Cisco ISE allows you to check only the version of the antimalware definition file using the Check against latest AV definition file version, if available option.</td>
</tr>
</tbody>
</table>
### Field

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Days Older Than</td>
<td>Define the number of days that the latest antimalware definition file date on the client can be older from the latest antimalware definition file date of the product or the current system date. The default value is zero (0).</td>
</tr>
<tr>
<td>Latest File Date</td>
<td>Choose to check the antimalware definition file date on the client, which can be older by the number of days that you define in the days older than field. If you set the number of days to the default value (0), then the antimalware definition file date on the client should not be older than the latest antimalware definition file date of the product. This check will work only if there is a value listed in Cisco ISE for the Latest Definition Date field for the selected product. Otherwise, the Current System Date field must be used.</td>
</tr>
<tr>
<td>Current System Date</td>
<td>Choose to check the antimalware definition file date on the client, which can be older by the number of days that you define in the days older than field. If you set the number of days to the default value (0), then the antimalware definition file date on the client should not be older than the current system date.</td>
</tr>
<tr>
<td>Products for Selected Vendor</td>
<td>Choose an antimalware product from the table. Based on the vendor that you select in the New Antimalware Condition page, the table retrieves information on their antimalware products and their version, remediation support that they provide, latest definition file date and its version. The selection of a product from the table allows you to check for the installation of an antimalware program, or check for the latest antimalware definition file date, and its latest version.</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Compound Posture Conditions](#), on page 562

### Dictionary Simple Condition Settings

The following table describes the fields in the Dictionary Simple Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Dictionary Simple Condition.
Table 144: Dictionary Simple Condition Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the dictionary simple condition that you want to create.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description of the dictionary simple condition that you want to create.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Choose an attribute from the dictionary.</td>
</tr>
<tr>
<td>Operator</td>
<td>Choose an operator to associate a value to the attribute that you have selected.</td>
</tr>
<tr>
<td>Value</td>
<td>Enter a value that you want to associate to the dictionary attribute, or choose a predefined value from the drop-down list.</td>
</tr>
</tbody>
</table>

Related Topics
- Dictionaries and Dictionary Attributes, on page 261
- Simple and Compound Conditions, on page 557
- Simple Posture Conditions, on page 561
- Create Simple Posture Conditions, on page 562

Dictionary Compound Condition Settings

The following table describes the fields in the Dictionary Compound Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Posture > Dictionary Compound Condition.

Table 145: Dictionary Compound Condition Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the dictionary compound condition that you want to create.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description of the dictionary compound condition that you want to create.</td>
</tr>
<tr>
<td>Select Existing Condition from Library</td>
<td>Define an expression by selecting pre-defined conditions from the policy elements library or add ad-hoc attribute/value pairs to your expression in the subsequent steps.</td>
</tr>
<tr>
<td>Condition Name</td>
<td>Choose dictionary simple conditions that you have already created from the policy elements library.</td>
</tr>
<tr>
<td>Expression</td>
<td>The Expression is updated based on your selection from the Condition Name drop-down list.</td>
</tr>
</tbody>
</table>
### Patch Management Condition Settings

The following table describes the fields in the Patch Management Conditions page. The navigation path is: Policy > Policy Elements > Conditions > Posture > Patch Management Condition.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the patch management condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the patch management condition.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Dictionary and Dictionary Attributes, on page 261
- Simple and Compound Conditions, on page 557
- Compound Posture Conditions, on page 562
- Create Compound Posture Conditions, on page 564
### Usage Guidelines

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Select an operating system to check the installation of a patch management software on the endpoint, or check the latest patch management definition file updates to which the condition is applied. You can select the Windows OS or Mac OS X. You can also select more than one version of an operating system to create the patch management condition.</td>
</tr>
<tr>
<td>Vendor Name</td>
<td>Choose a vendor name from the drop-down list. The patch management products of a vendor, and their supported version, check type, and minimum compliant module support are retrieved and displayed in the Products for Selected Vendor table. The list in the table changes according to the selected operating system.</td>
</tr>
</tbody>
</table>
### Fields

<table>
<thead>
<tr>
<th>Check Type</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Check Type</strong></td>
<td>Select any one of the following options:</td>
</tr>
<tr>
<td></td>
<td><strong>Installation</strong>—To check if the selected product is installed on the endpoint. This check type is supported by all vendors.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> For the Cisco Temporal Agent, you can only view Patch Management conditions containing the Installation check type in the Requirements page.</td>
</tr>
<tr>
<td></td>
<td><strong>Enabled</strong>—To check if the selected product is enabled on the endpoint. Verify if the vendor's product supports the chosen check type by referring to the Products for Selected Vendor list.</td>
</tr>
<tr>
<td></td>
<td><strong>Up to Date</strong>—To check if the selected product does not have missing patches. Verify if the vendor's product supports the chosen check type by referring to the Products for Selected Vendor list.</td>
</tr>
</tbody>
</table>

Click the Products for Selected Vendor drop-down arrow, to view the list of products that the vendor you have specified in the Vendor Name supports. For example, if you have selected Vendor A, that has two products, namely Product 1 and Product 2. Product 1 may support the Enabled option, whereas Product 2 might not. Or, if Product 1 does not support any of the check types, it is grayed out.

**Note** (Applicable for Cisco ISE 2.3 and above, and AnyConnect 4.5 and above) If you select the Up to Date Check Type in the Patch Management condition with SCCM, Cisco ISE

1. Uses the Microsoft API to check the current security patch for the specified severity level.

2. Triggers the Patch Management remediation for that missing security patch.
Check Patches Installed  

(Available only when you select the Up To Date check type.) You can configure severity levels for missing patches, which are then deployed based on the severity. Select any one of the severity levels:

- **Critical Only**—To check if critical software patches are installed on endpoints in your deployment.
- **Important & Critical**—To check if important and critical software patches are installed on endpoints in your deployment.
- **Moderate, Important, & Critical**—To check if moderate, important, and critical software patches are installed on endpoints in your deployment.
- **Low To Critical**—To check if low, moderate, important, and critical software patches are installed on endpoints in your deployment.
- **All**—To install the missing patches for all severity levels.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Patches Installed</td>
<td>(Available only when you select the Up To Date check type.) You can configure severity levels for missing patches, which are then deployed based on the severity. Select any one of the severity levels:</td>
</tr>
</tbody>
</table>

**Related Topics**

- Install a Software Patch, on page 88
- Roll Back Software Patches, on page 88
- View Patch Install and Rollback Changes
- Create Patch Management Conditions, on page 565

**Disk Encryption Condition Settings**

The following table describes the fields in the Disk Encryption Condition page. The navigation path is: Policy > Policy Elements > Conditions > Posture > Disk Encryption Condition.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the disk encryption condition that you want to create.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the disk encryption condition.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Select an operating system of the endpoint, whose disk is to be checked for encryption. You can select the Windows OS or Mac OS X. You can also select more than one version of an operating system to create the disk encryption condition.</td>
</tr>
</tbody>
</table>
**Usage Guidelines**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Name</td>
<td>Choose a vendor name from the drop-down list. The data encryption products of a vendor, and their supported version, the encryption state check, and the minimum compliant module support are retrieved and displayed in the <strong>Products for Selected Vendor</strong> table. The list in the table changes according to the selected operating system.</td>
</tr>
</tbody>
</table>
| Location             | Enabled only when an option is checked in the **Products for Selected Vendor** section. Select any one of the following options:  
  
  - **Specific Location**—To check if the specified disk drive is encrypted in the endpoint, (for example, C: for Windows OS) or a specified volume label is encrypted, (for example, Mackintosh HD for Mac OS X).  
  
  - **System Location**—To check if the default Windows OS system drive or Mac OS X hard drive is encrypted in the endpoint. |
| Encryption State     | The Encryption State checkbox is disabled when the selected product does not support encryption state check. The repeater is displayed only when the checkbox is checked. You can select the Fully Encrypted option to check if the client's disk drive is wholly encrypted. If you create a condition, for example for TrendMicro, and select two vendors—one with the Encryption State "Yes" and another with the Encryption State "No", then the Encryption State will be disabled because one of the Vendor Encryption State is "No".  
  
  **Note** You can click the repeater to add more Locations and the relationship between each location is the logical AND operator. |

**Related Topics**

- Create Disk Encryption Conditions, on page 565

**USB Condition Settings**

The following table describes the fields in the USB Condition page. The navigation path is: Work Centers > Posture > Policy Elements > USB. You can also navigate to the Policy > Policy Elements > Conditions > Posture > USB Condition page.

The USB check is a pre-defined condition and supports only Windows OS.
Table 148: USB Condition Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>USB_Check</td>
</tr>
<tr>
<td>Description</td>
<td>Cisco pre-defined check</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows</td>
</tr>
<tr>
<td>Compliance Module</td>
<td>A display-only field for ISE posture compliance module support for version 4.x (and later).</td>
</tr>
</tbody>
</table>

Related Topics

Simple Posture Conditions, on page 561

Hardware Attributes Condition Settings

Choose Policy > Policy Elements > Hardware Attributes Condition to access the Hardware Attributes Condition page. The following table describes the fields in the Hardware Attributes Condition page.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Hardware_Attributes_Check-The default name assigned to the condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Cisco pre-defined check that collects hardware attributes from clients.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows All or Mac OS</td>
</tr>
<tr>
<td>Compliance Module</td>
<td>4.x or later</td>
</tr>
</tbody>
</table>

Related Topics

The Hardware Dashboard, on page 20

Time and Date Condition Settings

The following table describes the fields in the Time and Date Conditions page. The navigation path for this page is: Policy > Policy Elements > Conditions > Common > Time and Date.

Table 149: Time and Date Condition Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Condition Name</td>
<td>Enter the name of the time and date condition.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the time and date condition.</td>
</tr>
<tr>
<td>Standard Settings</td>
<td></td>
</tr>
<tr>
<td>All Day</td>
<td>(Default) Set for the entire day.</td>
</tr>
<tr>
<td>Specific Hours</td>
<td>Configure hours, minutes, and AM/PM to set a to-and-from time range.</td>
</tr>
</tbody>
</table>
### Results

This section describes requirements for Cisco ISE services.

### Allowed Protocols

The following table describes the fields in the Allowed Protocols page, which allows you to configure the protocols to be used during authentication. The navigation path for this page is: Policy > Policy Elements > Results > Authentication > Allowed Protocols.

In the following table, PAC stands for Protected Access Credentials.

**Table 150: Allowed Protocols**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allowed Protocols &gt; Authentication Bypass</td>
<td></td>
</tr>
</tbody>
</table>
### Usage Guidelines

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Host Lookup</td>
<td>Check this check box if you want Cisco ISE to process the Host Lookup request. The Host Lookup request is processed for PAP/CHAP protocol when the RADIUS Service-Type equals 10 (Call-Check) and the username is equal to Calling-Station-ID. The Host Lookup request is processed for EAP-MD5 protocol when the Service-Type equals 1 (Framed) and the username is equal to Calling-Station-ID. Uncheck this check box if you want Cisco ISE to ignore the Host Lookup request and use the original value of the system username attribute for authentication. When unchecked, message processing is done according to the protocol (for example, PAP). Note: Unchecking the Process Host Lookup box could result in the failure of existing MAB authentications.</td>
</tr>
</tbody>
</table>

### Allowed Protocols > Authentication Protocols

<table>
<thead>
<tr>
<th>Allowed Protocols &gt; Authentication Protocols</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow PAP/ASCII</td>
<td>This option enables PAP/ASCII. PAP uses cleartext passwords (that is, unencrypted passwords) and is the least secure authentication protocol.</td>
</tr>
<tr>
<td>Allow CHAP</td>
<td>This option enables CHAP authentication. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with Microsoft Active Directory.</td>
</tr>
<tr>
<td>Allow MS-CHAPv1</td>
<td>Check this check box to enable MS-CHAPv1.</td>
</tr>
<tr>
<td>Allow MS-CHAPv2</td>
<td>Check this check box to enable MS-CHAPv2.</td>
</tr>
<tr>
<td>Allow EAP-MD5</td>
<td>Check this check box to enable EAP-based MD5 password hashed authentication.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Allow EAP-TLS | Check this check box to enable EAP-TLS Authentication protocol and configures EAP-TLS settings. You can specify how Cisco ISE will verify the user identity as presented in the EAP identity response from the end-user client. User identity is verified against information in the certificate that the end-user client presents. This comparison occurs after an EAP-TLS tunnel is established between Cisco ISE and the end-user client.  
  
  **Note**  
  
  EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps to configure certificates.  
  
  • Allow authentication of expired certificates to allow certificate renewal in Authorization Policy—Check this check box, if you want to allow users to renew certificates. If you check this check box, ensure that you configure appropriate authorization policy rules to check if the certificate has been renewed before processing the request any further.  
  
  • Enable Stateless Session Resume—Check this check box to allow EAP-TLS session resumption without requiring the session state to be stored at the server. Cisco ISE supports session ticket extension as described in RFC 5077. Cisco ISE creates a ticket and sends it to an EAP-TLS client. The client presents the ticket to ISE to resume a session.  
  
  • Proactive Session Ticket update—Enter the value as a percentage to indicate how much of the Time To Live (TTL) must elapse before the session ticket is updated. For example, if you enter the value 60, the session ticket is updated after 60 percent of the TTL has expired.  
  
  • Session ticket Time to Live—Enter the time after which the session ticket expires. This value determines the duration that a session ticket remains active. You can enter the value in seconds, minutes, hours, days, or weeks.  
<p>|
| Allow LEAP   | Check this check box to enable Lightweight Extensible Authentication Protocol (LEAP) authentication.                                            |</p>
<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow PEAP</td>
<td></td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>Check this check box to enable PEAP authentication protocol and PEAP settings. The default inner method is MS-CHAPv2. When you check the Allow PEAP check box, you can configure the following PEAP inner methods:</td>
</tr>
<tr>
<td></td>
<td>• Allow EAP-MS-CHAPv2—Check this check box to use EAP-MS-CHAPv2 as the inner method.</td>
</tr>
<tr>
<td></td>
<td>• Allow Password Change—Check this check box for Cisco ISE to support password changes.</td>
</tr>
<tr>
<td></td>
<td>• Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0 to 3.</td>
</tr>
<tr>
<td></td>
<td>• Allow EAP-GTC—Check this check box to use EAP-GTC as the inner method.</td>
</tr>
<tr>
<td></td>
<td>• Allow Password Change—Check this check box for Cisco ISE to support password changes.</td>
</tr>
<tr>
<td></td>
<td>• Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0 to 3.</td>
</tr>
<tr>
<td></td>
<td>• Allow EAP-TLS—Check this check box to use EAP-TLS as the inner method.</td>
</tr>
<tr>
<td></td>
<td>Check the <strong>Allow authentication of expired certificates to allow certificate renewal in Authorization Policy</strong> check box, if you want to allow users to renew certificates. If you check this check box, ensure that you configure appropriate authorization policy rules to check if the certificate has been renewed before processing the request any further.</td>
</tr>
<tr>
<td></td>
<td>• Require cryptobinding TLV—Check this check box if you want both the EAP peer and the EAP server to participate in the inner and outer EAP authentications of the PEAP authentication.</td>
</tr>
<tr>
<td></td>
<td>• Allow PEAPv0 only for legacy clients—Check this check box to allow PEAP supplicants to negotiate using PEAPv0. Some legacy clients do not conform to the PEAPv1 protocol standards.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>To ensure that such PEAP conversations are not dropped, check this check box.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Allow EAP-FAST</td>
<td></td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
</tr>
<tr>
<td>Check this checkbox to enable EAP-FAST authentication protocol and EAP-FAST settings. The EAP-FAST protocol can support multiple internal protocols on the same server. The default inner method is MS-CHAPv2. When you check the Allow EAP-FAST check box, you can configure EAP-FAST as the inner method:</td>
<td></td>
</tr>
<tr>
<td>• Allow EAP-MS-CHAPv2</td>
<td></td>
</tr>
<tr>
<td>• Allow Password Change—Check this check box for Cisco ISE to support password changes.</td>
<td></td>
</tr>
<tr>
<td>• Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0-3.</td>
<td></td>
</tr>
<tr>
<td>• Allow EAP-GTC</td>
<td></td>
</tr>
<tr>
<td>Allow Password Change—Check this check box for Cisco ISE to support password changes. Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0-3.</td>
<td></td>
</tr>
<tr>
<td>• Use PACs—Choose this option to configure Cisco ISE to provision authorization PACs for EAP-FAST clients. Additional PAC options appear.</td>
<td></td>
</tr>
<tr>
<td>• Don't use PACs—Choose this option to configure Cisco ISE to use EAP-FAST without issuing or accepting any tunnel or machine PACs. All requests for PACs are ignored and Cisco ISE responds with a Success-TLV without a PAC. When you choose this option, you can configure Cisco ISE to perform machine authentication.</td>
<td></td>
</tr>
<tr>
<td>• Allow EAP-TLS—Check this check box to use EAP-TLS as the inner method. Check the Allow authentication of expired certificates to allow certificate renewal in Authorization Policy check box, if you want to allow users to renew certificates. If you check this check box, ensure that you configure appropriate authorization policy rules to check if the certificate has been renewed before processing the request any further.</td>
<td></td>
</tr>
<tr>
<td>• Enable EAP Chaining—Check this check box</td>
<td></td>
</tr>
</tbody>
</table>
### Usage Guidelines

To enable EAP chaining:

EAP chaining allows Cisco ISE to correlate the results of user and machine authentication and apply the appropriate authorization policy using the EAPChainingResult attribute.

EAP chaining requires a supplicant that supports EAP chaining on the client device. Choose the User and Machine Authentication option in the supplicant.

EAP chaining is available when you choose the EAP-FAST protocol (both in PAC based and PAC less mode).

For PAC-based authentication, you can use user authorization PAC or machine authorization PAC, or both to skip the inner method.

For certificate-based authentication, if you enable the Accept Client Certificate for Provisioning option for the EAP-FAST protocol (in the Allowed Protocol service), and if the endpoint (AnyConnect) is configured to send the user certificate inside the tunnel, then during tunnel establishment, ISE authenticates the user using the certificate (the inner method is skipped), and machine authentication is done through the inner method. If these options are not configured, EAP-TLS is used as the inner method for user authentication.

After you enable EAP chaining, update your authorization policy and add a condition using the NetworkAccess:EapChainingResult attribute and assign appropriate permissions. For example:

- If EapChainingResult equal User and machine both succeeded - Full access
- If EapChainingResult equal User passed and machine failed - Restricted access
- If EapChainingResult equal User failed and machine passed - Restricted access
- If EapChainingResult equal User and machine both failed - Authentication fails. Cisco ISE does not process the authorization policy and sends a reject access message.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP chaining</td>
<td>Enables Cisco ISE to correlate the results of user and machine authentication.</td>
</tr>
<tr>
<td>EAP-FAST protocol</td>
<td>Available when User and Machine Authentication option is chosen.</td>
</tr>
<tr>
<td>PAC-based authentication</td>
<td>User or machine authorization PAC can be used to skip the inner method.</td>
</tr>
<tr>
<td>Certificate-based authentication</td>
<td>Accept Client Certificate for Provisioning enabled, certificate in tunnel.</td>
</tr>
<tr>
<td>Authorization policy update</td>
<td>EapChainingResult attribute added to authorization policy.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Full access, Restricted access, Authentication fails.</td>
</tr>
</tbody>
</table>

---

**Cisco Identity Services Engine Administrator Guide, Release 2.2**
<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow EAP-TTLS</td>
<td>Check this check box to enable EAP-TTLS protocol. You can configure the following inner methods:</td>
</tr>
<tr>
<td></td>
<td>• Allow PAP/ASCII—Check this check box to use PAP/ASCII as the inner method. You can use EAP-TTLS PAP for token and OTP-based authentications.</td>
</tr>
<tr>
<td></td>
<td>• Allow CHAP—Check this check box to use CHAP as the inner method. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with Microsoft Active Directory.</td>
</tr>
<tr>
<td></td>
<td>• Allow MS-CHAPv1—Check this check box to use MS-CHAPv1 as the inner method.</td>
</tr>
<tr>
<td></td>
<td>• Allow MS-CHAPv2—Check this check box to use MS-CHAPv2 as the inner method.</td>
</tr>
<tr>
<td></td>
<td>• Allow EAP-MD5—Check this check box to use EAP-MD5 as the inner method.</td>
</tr>
<tr>
<td></td>
<td>• Allow EAP-MS-CHAPv2—Check this check box to use EAP-MS-CHAPv2 as the inner method.</td>
</tr>
<tr>
<td></td>
<td>• Allow Password Change—Check this check box for Cisco ISE to support password changes.</td>
</tr>
<tr>
<td></td>
<td>• Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0 to 3.</td>
</tr>
<tr>
<td>Preferred EAP Protocol</td>
<td>Check this check box to choose your preferred EAP protocols from any of the following options: EAP-FAST, PEAP, LEAP, EAP-TLS, EAP-TTLS, and EAP-MD5. If you do not specify the preferred protocol, EAP-TLS is used by default.</td>
</tr>
<tr>
<td>EAP-TLS L-bit</td>
<td>Check this check box to support legacy EAP supplicants that expect L-bit flag (length- included flag) by default in TLS Change Cipher Spec message and Encrypted Handshake message from ISE.</td>
</tr>
</tbody>
</table>
### Fields

<table>
<thead>
<tr>
<th>Allow Weak Ciphers for EAP</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>If this option is enabled, legacy clients are allowed to negotiate using weak ciphers (such as RSA_RC4_128_SHA, RSA_RC4_128_MD5). We recommend that you enable this option only if your legacy clients support only weak ciphers. This option is disabled by default.</td>
<td></td>
</tr>
</tbody>
</table>

**Note** Cisco ISE does not support EDH_RSA_DES_64_CBC_SHA and EDH_DSS_DES_64_CBC_SHA.

<table>
<thead>
<tr>
<th>Require Message Authenticator for all RADIUS Requests</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>If this option is enabled, Cisco ISE verifies whether the RADIUS Message Authenticator attribute is present in the RADIUS message. If the message authenticator attribute is not present, the RADIUS message is discarded. Enabling this option provides protection from spoofed Access-Request messages and RADIUS message tampering. The RADIUS Message Authenticator attribute is a Message Digest 5 (MD5) hash of the entire RADIUS message.</td>
<td></td>
</tr>
</tbody>
</table>

**Note** EAP uses the Message Authenticator attribute by default and does not require that you enable it.

### Related Topics
- [Allowed Protocols in FIPS and Non-FIPS Modes for TACACS+ Device Administration](#), on page 200
- [Define Allowed Protocols for Network Access](#), on page 584

### PAC Options

The following table describes the fields after you select Use PACs in the Allowed Protocols Services List page. The navigation path for this page is: **Policy > Policy Elements > Results > Authentication > Allowed Protocols.**
<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use PAC</td>
<td></td>
</tr>
</tbody>
</table>
### PAC Options

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Tunnel PAC Time To Live—The Time to Live (TTL) value restricts the lifetime of the PAC. Specify the lifetime value and units. The default is 90 days. The range is between 1 and 1825 days.</td>
<td></td>
</tr>
<tr>
<td>• Proactive PAC Update When: &lt;n%&gt; of PAC TTL is Left—The Update value ensures that the client has a valid PAC. Cisco ISE initiates an update after the first successful authentication but before the expiration time that is set by the TTL. The update value is a percentage of the remaining time in the TTL. The default is 90%.</td>
<td></td>
</tr>
<tr>
<td>• Allow Anonymous In-band PAC Provisioning—Check this check box for Cisco ISE to establish a secure anonymous TLS handshake with the client and provision it with a PAC by using phase zero of EAP-FAST with EAP-MSCHAPv2. To enable anonymous PAC provisioning, you must choose both of the inner methods, EAP-MSCHAPv2 and EAP-GTC.</td>
<td></td>
</tr>
<tr>
<td>• Allow Authenticated In-band PAC Provisioning—Cisco ISE uses SSL server-side authentication to provision the client with a PAC during phase zero of EAP-FAST. This option is more secure than anonymous provisioning but requires that a server certificate and a trusted root CA be installed on Cisco ISE. When you check this option, you can configure Cisco ISE to return an Access-Accept message to the client after successful authenticated PAC provisioning.</td>
<td></td>
</tr>
<tr>
<td>• Server Returns Access Accept After Authenticated Provisioning—Check this check box if you want Cisco ISE to return an access-accept package after authenticated PAC provisioning.</td>
<td></td>
</tr>
<tr>
<td>• Allow Machine Authentication—Check this check box for Cisco ISE to provision an end-user client with a machine PAC and perform machine authentication (for end-user clients who do not have the machine credentials). The machine PAC can be provisioned to the client by request (in-band) or by the administrator (out-of-band). When Cisco ISE receives a valid machine PAC from the end-user client, the machine identity</td>
<td></td>
</tr>
</tbody>
</table>
Authorization Profile Settings

The following table describes the fields in the Standard Authorization Profiles page. The navigation path for this page is: Policy > Policy Elements > Results > Authorization > Authorization Profiles.

**Table 152: Authorization Profile settings**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name that identifies the new authorization profile.</td>
</tr>
</tbody>
</table>
## Authorization Profile Settings

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a description of the authorization profile.</td>
</tr>
<tr>
<td>Access Type</td>
<td>Choose the access type options (ACCESS_ACCEPT or ACCESS_REJECT).</td>
</tr>
<tr>
<td>Service Template</td>
<td>Check the check box to enable Cisco ISE to support sessions connecting from SANet capable devices. ISE implements service templates as authorization profiles that contain a special flag that marks them as “Service Template” compatible. This way, the service template, which is also an authorization profile, can be used in a single policy to support connection with SANet as well as non-SANet devices.</td>
</tr>
</tbody>
</table>

### Common Tasks

<table>
<thead>
<tr>
<th>DACL Name</th>
<th>You can use the default values (PERMIT_ALL_TRAFFIC or DENY_ALL_TRAFFIC), or select an attribute from the following dictionaries:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• External identity store (attributes)</td>
</tr>
<tr>
<td></td>
<td>• Endpoints</td>
</tr>
<tr>
<td></td>
<td>• Internal User</td>
</tr>
<tr>
<td></td>
<td>• Internal Endpoint</td>
</tr>
<tr>
<td></td>
<td>To add additional DACLs or edit and manage existing DACLs, see Downloadable ACLs, on page 617</td>
</tr>
<tr>
<td>VLAN</td>
<td>Check the check box and enter an attribute value that identifies a virtual LAN (VLAN) ID that you want associated with the new authorization profile you are creating (both integer and string values are supported for the VLAN ID). The format for this entry would be Tunnel-Private-Group-ID:VLANnumber.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you do not select a VLAN ID, Cisco ISE uses a default value of VLAN ID = 1. For example, if you only entered 123 as your VLAN number, the Attributes Details pane reflects the following value: Tunnel-Private-Group-ID = 1:123.</td>
</tr>
<tr>
<td>Voice Domain Permission</td>
<td>Check the check box to enable the vendor-specific attribute (VSA) of “cisco-av-pair” to be associated with a value of “device-traffic-class=voice”. In a multi-domain authorization mode, if the network switch receives this VSA, the endpoint is placed on to a voice domain after authorization.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Posture Discovery</strong></td>
<td>Check the check box to enable a redirection process used for Posture discovery in Cisco ISE, and enter an ACL on the device that you want to associate with this authorization profile. For example, if the value you entered is acl119, this is reflected in the Attributes Details pane as: cisco-av-pair = url-redirect-acl = acl119. The Attributes Details pane also displays: cisco-av-pair = url-redirect=<a href="https://ip:8443/guestportal/gateway?sessionid=SessionValueIdValue&amp;action=cpp">https://ip:8443/guestportal/gateway?sessionid=SessionValueIdValue&amp;action=cpp</a>.</td>
</tr>
<tr>
<td><strong>Centralized Web Authentication</strong></td>
<td>Check the check box to enable a redirection process that is similar to Posture discovery, but it redirects guest user access requests to the Guest server in Cisco ISE. Enter an ACL on the device that you want to associate with this authorization profile, and select <strong>Default</strong> or <strong>Manual</strong> as the redirect option. For example, if the value you entered is acl-999, this is reflected in the Attributes Details pane as: cisco-av-pair = url-redirect-acl = acl-99. The Attributes Details pane also displays: cisco-av-pair = url-redirect=<a href="https://ip:8443/guestportal/gateway?sessionid=SessionValueIdValue&amp;action=cwa">https://ip:8443/guestportal/gateway?sessionid=SessionValueIdValue&amp;action=cwa</a>. Check the <strong>Static IP/Host Name</strong> check box to specify an exact IP address or hostname to which you want the user to be redirected to. If this check box is not checked, the user will be redirected to the FQDN of the policy service node that received this request.</td>
</tr>
<tr>
<td><strong>Web Redirection (CWA, DRW, MDM, NSP, CPP)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Auto SmartPort</strong></td>
<td>Check the check box to enable Auto SmartPort functionality and enter a corresponding event name value in the text box. This enables the VSA cisco-av-pair with a value for this option as “auto-smart-port=event_name”. Your choice is reflected in the Attributes Details pane.</td>
</tr>
<tr>
<td><strong>Filter-ID</strong></td>
<td>Check the check box to enable a RADIUS filter attribute that sends the ACL name that you define in the text box (which is automatically appended with “.in”). Your choice is reflected in the Attributes Details pane.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Reauthentication</td>
<td>Check the check box and enter a value in seconds for maintaining connectivity during reauthentication. You can also choose attribute values from the Timer drop-down list. You choose to maintain connectivity during reauthentication by choosing to use either the default (a value of 0) or <strong>RADIUS-Request</strong> (a value of 1). Setting this to the RADIUS-Request value maintains connectivity during the reauthentication process.</td>
</tr>
<tr>
<td>MACSec Policy</td>
<td>Check the check box to enable the MACSec encryption policy whenever a MACSec-enabled client connects to Cisco ISE, and choose one of the following three options: <strong>must-secure</strong>, <strong>should-secure</strong>, or <strong>must-not-secure</strong>. For example, your choice is reflected in the Attributes Details pane as: cisco-av-pair = linksec-policy=must-secure.</td>
</tr>
<tr>
<td>NEAT</td>
<td>Check the check box to enable Network Edge Access Topology (NEAT), a feature that extends identity recognition between networks. Checking this check box displays the following value in the Attributes Details pane: cisco-av-pair = device-traffic-class=switch.</td>
</tr>
<tr>
<td>Interface Template</td>
<td>Check this check box and specify the template name to use an interface template for authentication. When you select this option, the following value is displayed in the Attributes Details pane: cisco-av-pair = interface-template-name=&lt;template_name&gt;.</td>
</tr>
<tr>
<td>Web Authentication (Local Web Auth)</td>
<td>Check the check box to enable local web authentication for this authorization profile. This value lets the switch recognize authorization for web authentication by Cisco ISE sending a VSA along with a DACL. The VSA is cisco-av-pair = priv-lvl=15 and this is reflected in the Attributes Details pane.</td>
</tr>
<tr>
<td>Wireless LAN Controller (WLC)</td>
<td>Check the check box and enter an ACL name in the text field. This value is used in a required Airespace VSA to authorize the addition of a locally defined ACL to a connection on the WLC. For example, if you entered rsa-1188, this would be reflected in the Attributes Details pane as: Airespace-ACL-Name = rsa-1188.</td>
</tr>
<tr>
<td>ASA VPN</td>
<td>Check the check box to enable an Adaptive Security Appliances (ASA) VPN group policy. From the Attribute list, choose a value to configure this setting.</td>
</tr>
</tbody>
</table>
### Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dictionaries</td>
<td>Click the down-arrow icon to display the available options in the Dictionaries window. Click to select the desired dictionary and attribute to configure in the first field.</td>
</tr>
<tr>
<td>Attribute Values</td>
<td>Click the down-arrow icon to display the available options in the Attribute Values window. Click to select the desired attribute group and attribute value for the second field. This value matches the one selected in the first field. Any Advanced Attributes setting(s) that you configure will be displayed in the Attribute Details panel.</td>
</tr>
<tr>
<td>Attributes Details</td>
<td>This pane displays any of the configured attribute values that you set for the Common Tasks and Advanced Attributes.</td>
</tr>
</tbody>
</table>

**Note**

To modify or delete any of the read-only values that are displayed in the Attributes Details pane, you must modify or delete these values in the corresponding Common Tasks field or in the attribute that you selected in the Attribute Values text box in the Advanced Attributes Settings pane.

**Note**

The values displayed in the Attributes Details pane are read-only and cannot be edited or deleted in this pane.

---

**Note**

For Client Provisioning without URL redirection, you can restrict the users to go to a specific VLAN to provide limited access. You must uncheck the Web Redirection checkbox and check the VLAN checkbox to configure the VLAN.

**Related Topics**

- Cisco ISE Authorization Profiles, on page 607
- Permissions for Authorization Profiles, on page 616
- Configure an Authorization Profile for Redirecting Nonregistered Devices, on page 257
- Create Authorization Profiles, on page 472

---

**Profiling Exception Action Settings**

The following table describes the fields in the New Profiler Exception Action page. The navigation path for this page is: **Policy > Policy Elements > Results > Profiling > Exception Actions.**
Table 153: Creating an Exception Action

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the exception action that you want to create.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description of the exception action that you want to create.</td>
</tr>
<tr>
<td>CoA Action to enforce CoA</td>
<td>Check the <strong>CoA Action</strong> check box to enforce CoA. When you associate an exception action in the endpoint profiling policy and enforce a CoA, you must configure CoA globally in Cisco ISE that can be done in the following location: Administration &gt; System &gt; Settings &gt; Profiling.</td>
</tr>
<tr>
<td>Policy Assignment</td>
<td>Click the <strong>Policy Assignment</strong> drop-down list that displays endpoint profiling policies that are configured in Cisco ISE, and choose the profiling policy against which the endpoint will be profiled when the exception action is triggered, regardless of its matched value.</td>
</tr>
<tr>
<td>System Type</td>
<td>Exception Actions can be any one of the following types:</td>
</tr>
<tr>
<td></td>
<td>• Cisco Provided—Includes AuthorizationChange, EndpointDelete, and FirstTimeProfile</td>
</tr>
<tr>
<td></td>
<td>• Administrator Created—Includes that are created by you as an administrator of Cisco ISE.</td>
</tr>
</tbody>
</table>

Related Topics

- **Profiling Exception Actions**, on page 688
- **Create Exception Actions**, on page 688

File Remediation

The following table describes the fields in the File Remediation page. The navigation path is: Policy > Policy Elements > Results > Posture > Remediation Actions > File Remediation.

Table 154: File Remediation

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>File Remediation Name</td>
<td>Enter a name for the file remediation. Once created and saved, you cannot edit the name of the file remediation.</td>
</tr>
<tr>
<td>File Remediation Description</td>
<td>Enter a description for the file remediation.</td>
</tr>
</tbody>
</table>
Usage Guidelines

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Enter the file version.</td>
</tr>
<tr>
<td>File to upload</td>
<td>Click <strong>Browse</strong> to locate the name of the file to be uploaded to the Cisco ISE server. This is the file that will be downloaded to the client when the file remediation action is triggered.</td>
</tr>
</tbody>
</table>

**Related Topics**

*Add a File Remediation*, on page 793

---

**Firewall Remediations**

The following table describes the fields on the Firewall Remediation page. The navigation path is: **Policy** > **Policy Elements** > **Results** > **Posture** > **Remediation Actions** > **Firewall Remediations**.

*Table 155: Firewall Remediations*

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the Firewall remediation.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description for the Firewall remediation.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Choose the Windows OS or Mac OSX.</td>
</tr>
<tr>
<td>Compliance Module</td>
<td>Support for OESIS version 4.x or later.</td>
</tr>
<tr>
<td>Remediation Type</td>
<td>Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Automatic</strong>—Enter values for the Interval and Retry Count. The ISE server identifies noncompliant clients and selects a remediation notification method and automatically updates the Firewall application on the client.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Manual</strong>—(Interval and Retry Count fields are disabled) Noncompliant clients should manually download and apply the latest Firewall application.</td>
</tr>
<tr>
<td>Interval (in seconds)</td>
<td>(Available only when you select the Automatic remediation type) Enter the time interval in seconds after which a scheduled patch update on the client is performed. Valid range is 0 to 9999.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>(Available only when you select the Automatic remediation type) Enter the number of times that a client can attempt to update critical patches. Valid range is 0 to 99.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

#### Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Name</td>
<td>Choose a vendor name (for example, VMware Inc.) from the drop-down list.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Supported versions of Cisco ISE and AnyConnect:</td>
</tr>
<tr>
<td></td>
<td>- Cisco ISE version 2.2 and later</td>
</tr>
<tr>
<td></td>
<td>- AnyConnect version 4.4 and later</td>
</tr>
<tr>
<td>Remediation Option</td>
<td><strong>Enable</strong>—Enables the Firewall application (if the vendor supports the enable option), in case it is disabled on the endpoint. Click the <strong>Products for Selected Vendor</strong> drop-down arrow, to view the list of products (for example, VMware vCentre Protect Agent), Version (for example, 8.x), and Enabled Remediation Support (for example, Yes) that the vendor you have specified in the <strong>Vendor Name</strong> supports. For example, if you have selected Vendor A, that has two products, namely Product 1 and Product 2. Product 1 may support the Enable remediation option, whereas Product 2 might not. The <strong>Products for Selected Vendor</strong> table changes according to the selected remediation option.</td>
</tr>
</tbody>
</table>

---

### Link Remediation

The following table describes the fields in the Link Remediation page. The navigation path is: **Policy > Policy Elements > Results > Posture > Remediation Actions > Link Remediation.**

**Table 156: Link Remediation**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Remediation Name</td>
<td>Enter a name for link remediation.</td>
</tr>
<tr>
<td>Link Remediation Description</td>
<td>Enter a description for the link remediation.</td>
</tr>
<tr>
<td>Remediation Type</td>
<td>Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Automatic</strong>—When selected, you should enter values for the Interval and Retry Count.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Manual</strong>—When selected, Retry Count and Interval fields are not editable.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Enter the number of attempts that clients can try to remediate from the link.</td>
</tr>
</tbody>
</table>
**Application Remediation**

The following table describes the fields in the Application Remediation page. The navigation path is: Policy > Policy Elements > Results > Posture > Remediation Actions > Application Remediation.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the application remediation.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter the description for the application remediation.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Select the Windows OS or MAC OS X to which the application remediation condition should be applied.</td>
</tr>
<tr>
<td>Compliance Module</td>
<td>Support for OESIS version 4.x or later.</td>
</tr>
<tr>
<td>Remediation Type</td>
<td>Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Automatic</strong>—Enter values for the Interval and Retry Count. The ISE server identifies non-compliant clients and selects a remediation notification method and automatically updates the latest patch on the client.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Manual</strong>—(Interval and Retry Count fields are disabled) Non-compliant clients should manually download and apply the latest patches.</td>
</tr>
<tr>
<td>Interval (in seconds)</td>
<td>(Available only when you select the Automatic remediation type) Enter the time interval in seconds after which a scheduled patch update on the client is performed. Valid range is 0 to 9999.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>(Available only when you select the Automatic remediation type) Enter the number of times that a client can attempt to update critical patches. Valid range is 0 to 99.</td>
</tr>
</tbody>
</table>
Antimalware Remediation

The following table describes the fields in the AV Remediation page. The navigation path is Policy > Policy Elements > Results > Posture > Remediation Actions > AV Remediation.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor Name</td>
<td>Choose a vendor name from the drop-down list. The application name (for example, Internet Explorer), version, vendor (for example, Microsoft Corporation), running processes, and category (for example, anti-phishing) are displayed in the Products for Selected Vendor table.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Supported versions of Cisco ISE and AnyConnect:</td>
</tr>
<tr>
<td></td>
<td>• Cisco ISE version 2.2 and later</td>
</tr>
<tr>
<td></td>
<td>• AnyConnect version 4.4 and later</td>
</tr>
<tr>
<td>Remediation Option</td>
<td>Select any one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Uninstall</strong>—Uninstalls an application. For example, you observe that there are many endpoints that are running a malicious application in the Context Directory page. You can create a requirement that uninstalls the malicious application.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Kill Process</strong>—Kills the required running patch management process. For example, you observe that there are many endpoints that are running a malicious process in the Context Directory page. You can create a requirement that kills these malicious processes that are running.</td>
</tr>
<tr>
<td></td>
<td>Click the Products for Selected Vendor drop-down arrow, to view the list of products that the vendor you have specified in the Patch Management Vendor Name supports. For example, if you have selected Vendor A, that has two products, namely Product 1 and Product 2. Product 1 may support the Enable remediation option, whereas Product 2 might not. Or, if Product 1 does not support the Enable and Install missing patches remediation options, then Product 1 is disabled (grayed out). The Products for Selected Vendor table changes according to the selected remediation option.</td>
</tr>
</tbody>
</table>
**Table 158: Antivirus Remediation**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the antimalware remediation.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the antimalware remediation.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Windows</td>
</tr>
<tr>
<td></td>
<td>• Macintosh—when selected Remediation Type, Interval, and Retry Count fields are not editable</td>
</tr>
<tr>
<td>Compliance Module</td>
<td>OESIS version 4 supports compliance module 4.x and AnyConnect 4.3 and higher.</td>
</tr>
<tr>
<td>Remediation Type</td>
<td>Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Automatic—When selected, you should enter values for the Interval and Retry Count.</td>
</tr>
<tr>
<td></td>
<td>• Manual—When selected, Retry Count and Interval fields are not editable.</td>
</tr>
<tr>
<td>Interval (in seconds)</td>
<td>Enter the time interval in seconds that clients can try to remediate after previous attempts.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Enter the number of attempts that clients can try to update an antimalware definition.</td>
</tr>
<tr>
<td>Anti-Malware Vendor Name</td>
<td>Choose the required antimalware vendor.</td>
</tr>
</tbody>
</table>

**Related Topics**

Create Posture Requirement in Stealth Mode, on page 802

---

**Antivirus Remediation**

The following table describes the fields in the Anti-Virus Remediation page. The navigation path is Policy > Policy Elements > Results > Posture > Remediation Actions > Anti-Virus Remediation.

**Table 159: Anti-Virus Remediation**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the antivirus remediation.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the antivirus remediation.</td>
</tr>
</tbody>
</table>
### Antispyware Remediation

The following table describes the fields in the AS Remediation page. The navigation path is Policy > Policy Elements > Results > Posture > Remediation Actions > AS Remediation.

#### Table 160: Antispyware Remediation

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediation Type</td>
<td>Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Automatic</strong>—When selected, you should enter values for the Interval and Retry Count.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Manual</strong>—When selected, Retry Count and Interval fields are not editable.</td>
</tr>
<tr>
<td>Interval (in seconds)</td>
<td>Enter the time interval in seconds that clients can try to remediate after previous attempts.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Enter the number of attempts that clients can try to update an antivirus definition.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Windows</strong></td>
</tr>
<tr>
<td></td>
<td>• <strong>Macintosh</strong>—when selected Remediation Type, Interval, and Retry Count fields are not editable</td>
</tr>
<tr>
<td>AV Vendor Name</td>
<td>Choose the antivirus vendor.</td>
</tr>
</tbody>
</table>

**Related Topics**
- [Add an Antivirus Remediation](#), on page 794
- [Create Posture Requirement in Stealth Mode](#), on page 802
Launch Program Remediation

The following table describes the fields in the Launch Program Remediation page. The navigation path is: Policy > Policy Elements > Results > Posture > Remediation Actions > Launch Program Remediation.

### Table 161: Launch Program Remediation

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the launch program remediation.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the launch program remediation that you want to create.</td>
</tr>
<tr>
<td>Remediation Type</td>
<td>Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Automatic</strong>—When selected, you should enter the Retry Count and Interval options.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Manual</strong>—When selected, Interval and Retry Count fields are not editable.</td>
</tr>
<tr>
<td>Interval (in seconds)</td>
<td>Enter the time interval in seconds that clients can try to remediate after previous attempts.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Enter the number of attempts that clients can try to launch required programs.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Program Installation Path</td>
<td>From the drop-down list, choose the path where the remediation program has to be installed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>ABSOLUTE_PATH</strong> — remediation program is installed in the fully qualified path of the file. For example, C:&lt;directory&gt;\</td>
</tr>
<tr>
<td></td>
<td>• <strong>SYSTEM_32</strong> — remediation program is installed in the C:\WINDOWS\system32 directory</td>
</tr>
<tr>
<td></td>
<td>• <strong>SYSTEM_DRIVE</strong> — remediation program is installed in the C:\ drive</td>
</tr>
<tr>
<td></td>
<td>• <strong>SYSTEM_PROGRAMS</strong> — remediation program is installed in the C:\Program Files</td>
</tr>
<tr>
<td></td>
<td>• <strong>SYSTEM_ROOT</strong> — remediation program is installed in the root path of Windows system</td>
</tr>
<tr>
<td>Program Executable</td>
<td>Enter the name of the remediation program executable, or an installation file.</td>
</tr>
<tr>
<td>Program Parameters</td>
<td>Enter required parameters for the remediation programs.</td>
</tr>
<tr>
<td>Existing Programs</td>
<td>Existing Programs table displays the installation paths, name of the remediation programs, and parameters if any.</td>
</tr>
<tr>
<td></td>
<td>• Click Add to add remediation programs to the Existing Programs list.</td>
</tr>
<tr>
<td></td>
<td>• Click the delete icon to remove the remediation programs from the list.</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Add a Launch Program Remediation](#), on page 795
- [Troubleshoot Launch Program Remediation](#), on page 795
- [Create Posture Requirement in Stealth Mode](#), on page 802

**Windows Update Remediation**

The following table describes the fields in the Windows Update Remediation page. The navigation path is: Policy > Policy Elements > Results > Posture > Remediation Actions > Windows Update Remediation.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the Windows update remediation.</td>
</tr>
</tbody>
</table>
### Fields

<table>
<thead>
<tr>
<th>Description</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a description for the Windows update remediation.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Remediation Type</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose one of the following:</td>
<td></td>
</tr>
<tr>
<td>• Automatic—When selected, you should enter the Retry Count and Interval options.</td>
<td></td>
</tr>
<tr>
<td>• Manual—When selected, Interval and Retry Count fields are not editable.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interval (in seconds)</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the time interval in seconds that clients can try to remediate after previous attempts.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Retry Count</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter the number of attempts that Windows clients can try for Windows updates.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Windows Update Setting</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose from the following:</td>
<td></td>
</tr>
<tr>
<td>• Do not change setting—The Windows Automatic Updates client configuration does not change during or after Windows update remediation.</td>
<td></td>
</tr>
<tr>
<td>• Notify to download and install—Windows only notifies clients, but does not automatically download, or install them.</td>
<td></td>
</tr>
<tr>
<td>• Automatically download and notify to install—Windows downloads updates for clients, and notifies clients to install Windows updates.</td>
<td></td>
</tr>
<tr>
<td>• Automatically download and install—Windows automatically downloads, and installs Windows updates. This is the highly recommended setting for Windows clients.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Override User’s Windows Update setting with administrator’s</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check this check box to enforce the administrator-specified setting for Windows Automatic Updates on all the clients during, and after Windows update remediation.</td>
<td></td>
</tr>
</tbody>
</table>

If unchecked, the setting enforces the following:

- The administrator-specified setting only when Automatic Updates are disabled on Windows clients.
- The Windows clients-specified setting only when Windows Automatic Updates are enabled on the client.
Windows Server Update Services Remediation

The following table describes the fields in the Windows Update Remediation page. The navigation path is: Policy > Policy Elements > Results > Posture > Remediation Actions > Windows Server Update Services Remediation.

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the WSUS remediation.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the WSUS remediation.</td>
</tr>
<tr>
<td>Remediation Type</td>
<td>Choose from the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Automatic</strong>—The NAC Agents automatically updates Windows clients with the latest WSUS updates.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Manual</strong>—If selected, the Interval and Retry Count fields are not editable. The user manually updates the Windows client with the latest WSUS updates from a Microsoft-managed WSUS server, or from the locally administered WSUS server for compliance.</td>
</tr>
<tr>
<td>Interval (in seconds)</td>
<td>Enter the interval in seconds (the default interval is 0) to delay WSUS updates before the NAC Agents and Web Agents attempt to retry after the previous attempt.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Enter the number of attempts that the NAC Agents and web Agents retry to update Windows clients with WSUS updates.</td>
</tr>
<tr>
<td>Validate Windows updates using</td>
<td>Choose from the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Cisco Rules</strong>—If you choose this option, you can select custom or preconfigured rules as conditions in the posture requirement</td>
</tr>
<tr>
<td></td>
<td>• <strong>Severity Level</strong>—If you choose this option, you can select custom or preconfigured rules as conditions in the posture requirement, but they are not used. The pr_WSUSRule can be used as a placeholder condition (a dummy condition) in the posture requirement that specifies a WSUS remediation.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Windows Updates Severity Level</td>
<td>Choose the severity level:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Critical</strong>—Installs only critical Windows updates</td>
</tr>
<tr>
<td></td>
<td>• <strong>Express</strong>—Installs important and critical Windows updates</td>
</tr>
<tr>
<td></td>
<td>• <strong>Medium</strong>—Installs all critical, important, and moderate Windows updates</td>
</tr>
<tr>
<td></td>
<td>• <strong>All</strong>—Installs all critical, important, moderate, and low Windows updates</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> When you associate a WSUS remediation action to a posture requirement to validate Windows updates by using the severity level option, you must choose the pr_WSUSRule (a dummy compound condition) compound condition in the posture requirement. When the posture requirement fails, the NAC Agent enforces the remediation action (Windows updates) based on the severity level that you define in the WSUS remediation.</td>
</tr>
<tr>
<td>Update to latest OS Service Pack</td>
<td>Check this check box to allow WSUS remediation install the latest service pack available for the client's operating system automatically.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The operating system service packs are updated automatically irrespective of the Medium and All severity level options selected in WSUS remediation.</td>
</tr>
<tr>
<td>Windows Updates Installation Source</td>
<td>Specifies the source from where you install WSUS updates on Windows clients:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Microsoft server</strong>—Microsoft-managed WSUS server</td>
</tr>
<tr>
<td></td>
<td>• <strong>Managed server</strong>—Locally administered WSUS server</td>
</tr>
</tbody>
</table>
### Patch Management Remediation

The following table describes the fields in the Patch Management Remediation page. The navigation path is: **Policy > Policy Elements > Results > Posture > Remediation Actions > Patch Management Remediation**.

**Table 164: Patch Management Remediation**

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the patch management remediation.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the patch management remediation.</td>
</tr>
<tr>
<td>Compliance Module</td>
<td>Support for OESIS version 4.x or later or 3.x or earlier.</td>
</tr>
<tr>
<td>Remediation Type</td>
<td>Choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Automatic</strong>—Enter values for the Interval and Retry Count. The ISE server identifies non-compliant clients and selects a remediation notification method and automatically updates the latest patch on the client.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Manual</strong>—(Interval and Retry Count fields are disabled) Non-compliant clients should download and apply the latest patches manually.</td>
</tr>
<tr>
<td>Fields</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Interval (in seconds)</td>
<td>(Available only when you select the Automatic remediation type) Enter the time interval in seconds after which a scheduled patch update on the client is performed.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>(Available only when you select the Automatic remediation type) Enter the number of times that a client can attempt to update critical patches.</td>
</tr>
<tr>
<td>Operating System</td>
<td>Windows OS is the only OS that is supported.</td>
</tr>
<tr>
<td>Patch Management Vendor Name</td>
<td>Choose a vendor name from the drop-down list. The patch management remediation products of a vendor along with their product's support for the version, enable remediation, update remediation, and show UI remediation is displayed in the <strong>Products for Selected Vendor</strong> table.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Supported versions of Cisco ISE and AnyConnect:</td>
</tr>
<tr>
<td></td>
<td>• Cisco ISE version 1.4 and later</td>
</tr>
<tr>
<td></td>
<td>• AnyConnect version 4.1 and later</td>
</tr>
<tr>
<td>Remediation Option</td>
<td>Select any one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable</strong>—Enables the patch management software, in case it is disabled on the endpoint.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Install Missing Patches</strong>—Updates the patch on the endpoint.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Activate Patch Management Software GUI</strong>—Displays the patch management software user interface. Follow the instructions on this page to change the software settings or initiate software updates.</td>
</tr>
<tr>
<td></td>
<td>Click the <strong>Products for Selected Vendor</strong> drop-down arrow, to view the list of products that the vendor you have specified in the <strong>Patch Management Vendor Name</strong> supports. For example, if you have selected Vendor A, that has two products, namely Product 1 and Product 2. Product 1 may support the Enable remediation option, whereas Product 2 might not. Or, if Product 1 does not support the Enable and Install missing patches remediation options, then Product 1 is disabled (grayed out). The <strong>Products for Selected Vendor</strong> table changes according to the selected remediation option.</td>
</tr>
</tbody>
</table>
### USB Mass Storage Check Workflow

You can use the USB_Check condition (Cisco predefined) in a posture policy to check if a USB mass storage device is connected to an endpoint. The USB mass storage check and remediation flow is described below.

The AnyConnect agent:

- Checks for a USB connection.
- Detects a USB plug-in and applies the USB_Block remediation (Cisco predefined). The AnyConnect agent reports a remediation failure to Cisco ISE and initiates a CoA. The USB mass storage remediation is always active and is not limited to the time of access or Periodic reassessment (PRA).
- Stops running the USB detection, when the user disconnects from the network interface.
- Runs the posture flow again, when the endpoint reconnects. However, if the endpoint is in the posture lease period, the AnyConnect agent does not run the USB check again.

### Related Topics

- **Add a Patch Management Remediation**, on page 793
- **Create Posture Requirement in Stealth Mode**, on page 802

### Usage Guidelines

You can configure severity levels for missing patch management remediation software, which are then deployed based on the severity. Select any one of the severity levels:

- **Critical Only**—To check if critical remediation software patches are installed on endpoints in your deployment.
- **Important & Critical**—To check if important and critical remediation software patches are installed on endpoints in your deployment.
- **Moderate, Important, & Critical**—To check if moderate, important, and critical remediation software patches are installed on endpoints in your deployment.
- **Low To Critical**—
- **All**—Checks all severity levels.
AnyConnect performs the USB check and remediation sequentially. Consequently, there may be a delay in handling USB dynamic change while performing PRA. When the USB check is configured, it is recommended to minimize the PRA grace time (Work Centers > Posture > Settings > Reassessment Configurations) for the other checks.

Note
You cannot create a compound condition for USB check.

Related Topics
- USB Condition Settings, on page 1114
- Simple Posture Conditions, on page 561

USB Mass Storage Remediation

The following table describes the fields in the USB Remediation page. The navigation path is: Work Centers > Posture > Policy Elements > Remediations > USB. You can also view the option in the Policy > Policy Elements > Results > Posture > Remediation Actions > USB Remediation page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guideline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name for the USB remediation.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the USB remediation.</td>
</tr>
<tr>
<td>Compliance Module</td>
<td>A display-only field for ISE posture compliance module support for version 4.x (and later).</td>
</tr>
<tr>
<td>Operating System</td>
<td>A display-only field to indicate support for Windows OS.</td>
</tr>
<tr>
<td>Remediation Type</td>
<td>A display-only field to indicate that the remediation is automatic.</td>
</tr>
<tr>
<td>Interval</td>
<td>Enter the time interval in seconds after which a scheduled USB mass storage device check on the client is performed.</td>
</tr>
<tr>
<td>Retry Count</td>
<td>Enter the time interval in seconds after which a USB mass storage device reassessment on the client is performed.</td>
</tr>
</tbody>
</table>

Related Topics
- Simple Posture Conditions, on page 561
Client Posture Requirements

The following table describes the fields in the Posture Requirements page. The navigation path is: Policy > Policy Elements > Results > Posture > Requirements.

Table 166: Posture Requirement

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the requirement.</td>
</tr>
<tr>
<td>Operating Systems</td>
<td>Choose an operating system. Click plus [+] to associate more than one operating system to the policy. Click minus [-] to remove the operating system from the policy.</td>
</tr>
<tr>
<td>Conditions</td>
<td>Choose a Condition from the list. You can also create any user defined condition by clicking the Action Icon and associate it with the requirement. You cannot edit the associated parent operating system while creating user defined conditions. The pr_WSUSRule is a dummy compound condition, which is used in a posture requirement with an associated Windows Server Update Services (WSUS) remediation. The associated WSUS remediation action must be configured to validate Windows updates by using the severity level option. When this requirement fails, the NAC Agent that is installed on the Windows client enforces the WSUS remediation action based on the severity level that you define in the WSUS remediation. The pr_WSUSRule cannot be viewed in the Compound conditions list page. You can only select the pr_WSUSRule from the Conditions widget.</td>
</tr>
</tbody>
</table>
### Fields
<table>
<thead>
<tr>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediation Actions</td>
</tr>
<tr>
<td>Choose a Remediation from the list. You can also create a remediation action and associate it with the requirement. You have a text box for all the remediation types that can be used to communicate to the Agent users. In addition to remediation actions, you can communicate to Agent users about the noncompliance of clients with messages. The <strong>Message Text Only</strong> option informs Agent users about the noncompliance. It also provides optional instructions to the user to contact the Help desk for more information, or to remediate the client manually. In this scenario, the NAC Agent does not trigger any remediation action.</td>
</tr>
</tbody>
</table>

### Related Topics
- [Configure Acceptable Use Policies for Posture Assessment](#), on page 780
- [Create Client Posture Requirements](#), on page 797
RADIUS Live Logs

The following table describes the fields in the RADIUS Live logs page, which displays the recent RADIUS authentications. The navigation path for this page is: Operations > RADIUS > Live Logs. You can view the RADIUS live logs only in the Primary PAN.

<table>
<thead>
<tr>
<th>Options</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>Shows the time that the log was received by the monitoring and troubleshooting collection agent. This column is required and cannot be deselected.</td>
</tr>
<tr>
<td>Status</td>
<td>Shows if the authentication was successful or a failure. This column is required and cannot be deselected. Green is used to represent passed authentications. Red is used to represent failed authentications.</td>
</tr>
<tr>
<td><strong>Usage Guidelines</strong></td>
<td><strong>Options</strong></td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Brings up a report when you click the magnifying glass icon, allowing you to drill down and view more detailed information on the selected authentication scenario. This column is required and cannot be deselected.</td>
<td>Details</td>
</tr>
<tr>
<td>You cannot view the details for endpoints that are active for more than 48 hours. You might see a page with the following message when you click the Details icon for endpoints that are active for more than 48 hours: No Data available for this record. Either the data is purged or authentication for this session record happened a week ago. Or if this is an 'PassiveID' or 'PassiveID Visibility' session, it will not have authentication details on ISE but only the session.</td>
<td></td>
</tr>
<tr>
<td>Shows the number of time the authentication requests were repeated in last 24 hours, without any change in the context of identity, network devices, and authorization</td>
<td>Repeat Count</td>
</tr>
<tr>
<td>Shows the logged in user name that is associated with the authentication.</td>
<td>Identity</td>
</tr>
<tr>
<td>Shows the unique identifier for an endpoint, usually a MAC or IP address.</td>
<td>Endpoint ID</td>
</tr>
<tr>
<td>Shows the type of endpoint that is profiled, for example, profiled to be an iPhone, Android, MacBook, Xbox, and so on.</td>
<td>Endpoint Profile</td>
</tr>
<tr>
<td>Shows the name of the policy selected for specific authentication.</td>
<td>Authentication Policy</td>
</tr>
<tr>
<td>Shows the name of the policy selected for specific authorization.</td>
<td>Authorization Policy</td>
</tr>
<tr>
<td>Shows an authorization profile that was used for authentication.</td>
<td>Authorization Profiles</td>
</tr>
<tr>
<td>Shows the IP address of the endpoint device.</td>
<td>IP Address</td>
</tr>
<tr>
<td>Shows the IP address of the Network Access Device.</td>
<td>Network Device</td>
</tr>
<tr>
<td>Shows the port number at which the endpoint is connected.</td>
<td>Device Port</td>
</tr>
</tbody>
</table>
### Options

<table>
<thead>
<tr>
<th>Identity Group</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Shows the identity group that is assigned to the user or endpoint, for which the log was generated.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Posture Status</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Shows the status of posture validation and details on the authentication.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Indicates the Policy Service from which the log was generated.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MDM Server Name</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Shows the names of the MDM servers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Shows the event status.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Failure Reason</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Shows a detailed reason for failure, if the authentication failed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Auth Method</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Shows the authentication method that is used by the RADIUS protocol, such as Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2), IEE 802.1x or dot1x, and the like.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authentication Protocol</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and the like.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Group</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Shows the group that is identified by the authentication log.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Session ID</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Shows the session ID.</td>
</tr>
</tbody>
</table>

---

**Note**

In the RADIUS Live Logs and TACACS+ Live Logs details page, a “Queried PIP” entry will appear for the first Attribute for each Policy authorization rule. If all the attributes within the authorization rule are related to a dictionary that was already queried for previous Rules, then no additional “Queried PIP” entry will appear.

You can do the following in the RADIUS Live Logs page:

- Export the data in csv or pdf format.
- Show or hide the columns based on your requirements.
- Filter the data using quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
- Sort the column values.

---

**Note**

All the user customizations will be stored as user preferences.
RADIUS Live Sessions

The following table describes the fields in the RADIUS Live Sessions page, which displays live authentications. The navigation path for this page is: Operations > RADIUS > Live Sessions. You can view the RADIUS live sessions only in the Primary PAN.

Table 168: RADIUS Live Sessions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initiated</td>
<td>Shows the timestamp when the session was initiated.</td>
</tr>
<tr>
<td>Updated</td>
<td>Shows the timestamp when the session was last updated due to any change.</td>
</tr>
<tr>
<td>Account Session Time</td>
<td>Shows the time span (in seconds) of a user's session.</td>
</tr>
<tr>
<td>Session Status</td>
<td>Shows the current status of the endpoint device.</td>
</tr>
<tr>
<td>Action</td>
<td>Click the Actions icon to re-authenticate an active RADIUS session or disconnect an active RADIUS session.</td>
</tr>
<tr>
<td>Repeat Count</td>
<td>Shows the number of times the user or endpoint is re-authenticated.</td>
</tr>
<tr>
<td>Endpoint ID</td>
<td>Shows the unique identifier for an endpoint, usually a MAC or IP address.</td>
</tr>
<tr>
<td>Identity</td>
<td>Shows the username of the endpoint device.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Shows the IP address of the endpoint device.</td>
</tr>
<tr>
<td>Audit Session ID</td>
<td>Shows a unique session identifier.</td>
</tr>
<tr>
<td>Account Session ID</td>
<td>Shows a unique ID provided by the network device.</td>
</tr>
<tr>
<td>Endpoint Profile</td>
<td>Shows the endpoint profile for the device.</td>
</tr>
<tr>
<td>Posture Status</td>
<td>Shows the status of posture validation and details on the authentication.</td>
</tr>
<tr>
<td>Security Group</td>
<td>Shows the group that is identified by the authentication log.</td>
</tr>
<tr>
<td>Server</td>
<td>Indicates the Policy Service node from which the log was generated.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Auth Method</td>
<td>Shows the authentication method that is used by the RADIUS protocol, such as Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), IEE 802.1x or dot1x, and the like.</td>
</tr>
<tr>
<td>Authentication Protocol</td>
<td>Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and the like.</td>
</tr>
<tr>
<td>Authentication Policy</td>
<td>Shows the name of the policy selected for specific authentication.</td>
</tr>
<tr>
<td>Authorization Policy</td>
<td>Shows the name of the policy selected for specific authorization.</td>
</tr>
<tr>
<td>Authorization Profiles</td>
<td>Shows an authorization profile that was used for authentication.</td>
</tr>
<tr>
<td>NAS IP Address</td>
<td>Shows IP address of the network devices.</td>
</tr>
<tr>
<td>Device Port</td>
<td>Shows the connected port to the network device.</td>
</tr>
<tr>
<td>PRA Action</td>
<td>Shows the periodic reassessment action taken on a client after it is successfully postured for compliance on your network.</td>
</tr>
<tr>
<td>ANC Status</td>
<td>Adaptive Network Control status of a device as Quarantine, Unquarantine, or Shutdown.</td>
</tr>
<tr>
<td>WLC Roam</td>
<td>Shows the boolean (Y/N) used to track that an endpoint has been handed off during roaming, from one WLC to another. It has the value of cisco-av-pair=nas-update = Y or N.</td>
</tr>
</tbody>
</table>

**Note** Cisco ISE relies on nas-update=true attribute from WLC to identify whether the session is in roaming state. When the original WLC sends an accounting stop attribute with nas-update=true, the session is not deleted in ISE to avoid reauthentication. If roaming fails due to some reason, ISE clears the session after 5 days of inactivity.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets In</td>
<td>Shows the number of packets received.</td>
</tr>
<tr>
<td>Packets Out</td>
<td>Shows the number of packets sent.</td>
</tr>
<tr>
<td>Bytes In</td>
<td>Shows the number of bytes received.</td>
</tr>
<tr>
<td>Bytes Out</td>
<td>Shows the number of bytes sent.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Session Source</td>
<td>Indicates whether it is a RADIUS session or PassiveID session.</td>
</tr>
<tr>
<td>User Domain Name</td>
<td>Shows the registered DNS name of the user.</td>
</tr>
<tr>
<td>Host Domain Name</td>
<td>Shows the registered DNS name of the host.</td>
</tr>
<tr>
<td>User NetBIOS Name</td>
<td>Shows the NetBIOS name of the user.</td>
</tr>
<tr>
<td>Host NetBIOS Name</td>
<td>Shows the NetBIOS name of the host.</td>
</tr>
<tr>
<td>License Type</td>
<td>Shows the type of license used—Base, Plus, Apex, or Plus and Apex.</td>
</tr>
<tr>
<td>License Details</td>
<td>Shows the license details.</td>
</tr>
<tr>
<td>Provider</td>
<td>Endpoint events are learned from different syslog sources. These syslog</td>
</tr>
<tr>
<td></td>
<td>sources are referred to as providers.</td>
</tr>
<tr>
<td></td>
<td>• Windows Management Instrumentation (WMI)—WMI is a Windows service that</td>
</tr>
<tr>
<td></td>
<td>provides a common interface and object model to access management</td>
</tr>
<tr>
<td></td>
<td>information about operating system, devices, applications, and services.</td>
</tr>
<tr>
<td></td>
<td>• Agent—A program that runs on a client on behalf of the client or another</td>
</tr>
<tr>
<td></td>
<td>program.</td>
</tr>
<tr>
<td></td>
<td>• Syslog—A logging server to which a client sends event messages.</td>
</tr>
<tr>
<td></td>
<td>• REST—A client is authenticated through a terminal server. The TS Agent ID,</td>
</tr>
<tr>
<td></td>
<td>Source Port Start, Source Port End, and Source First Port values are</td>
</tr>
<tr>
<td></td>
<td>displayed for this syslog source.</td>
</tr>
<tr>
<td></td>
<td>• Span—Network information is discovered using span probes.</td>
</tr>
<tr>
<td></td>
<td>• DHCP—DHCP event.</td>
</tr>
<tr>
<td></td>
<td>• Endpoint</td>
</tr>
<tr>
<td></td>
<td>When two events from different providers are learned from an endpoint</td>
</tr>
<tr>
<td></td>
<td>session, the providers are displayed as comma-separated values in the</td>
</tr>
<tr>
<td></td>
<td>live sessions page.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Shows the MAC address of a client.</td>
</tr>
<tr>
<td>Endpoint Check Time</td>
<td>Shows the time at which the endpoint was last checked by the endpoint probe.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Endpoint Check Result</td>
<td>Shows the result of an endpoint probe. The possible values are: • Unreachable • User Logout • Active User</td>
</tr>
<tr>
<td>Source Port Start</td>
<td>(Values are displayed only for the REST provider) Shows the first port number in a port range.</td>
</tr>
<tr>
<td>Source Port End</td>
<td>(Values are displayed only for the REST provider) Shows the last port number in a port range.</td>
</tr>
<tr>
<td>Source First Port</td>
<td>(Values are displayed only for the REST provider) Shows the first port allocated by the Terminal Server (TS) Agent.</td>
</tr>
<tr>
<td></td>
<td>A Terminal Server (TS) refers to a server or network device that allows multiple endpoints to connect to it without a modem or network interface and facilities the connection of the multiple endpoints to a LAN network. The multiple endpoints appear to have the same IP address and therefore it is difficult to identify the IP address of a specific user. Consequently, to identify a specific user, a TS Agent is installed in the server, which allocates a port range to each user. This helps create an IP address-port-user mapping.</td>
</tr>
<tr>
<td>TS Agent ID</td>
<td>(Values are displayed only for the REST provider) Shows the unique identity of the Terminal Server (TS) agent that is installed on an endpoint.</td>
</tr>
<tr>
<td>AD User Resolved Identities</td>
<td>(Values are displayed only for AD user) Shows the potential accounts that matched.</td>
</tr>
<tr>
<td>AD User Resolved DNs</td>
<td>(Values are displayed only for AD user) Shows the Distinguished Name of AD user, for example, CN=chris,CN=Users,DC=R1,DC=com</td>
</tr>
</tbody>
</table>

Related Topics

- Change Authorization for RADIUS Sessions, on page 910
- Cisco ISE Active RADIUS Sessions, on page 910

**TACACS Live Logs**

The following table describes the fields in the TACACS Live Logs page, which displays the TACACS+ AAA details. The navigation path for this page is: Operations > TACACS Live Logs. You can view the TACACS live logs only in the Primary PAN.
### Table 169: TACACS Live Logs

<table>
<thead>
<tr>
<th>Fields</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generated Time</td>
<td>Shows the syslog generation time based on when a particular event was triggered.</td>
</tr>
<tr>
<td>Logged Time</td>
<td>Shows the time when the syslog was processed and stored by the Monitoring node. This column is required and cannot be deselected.</td>
</tr>
<tr>
<td>Status</td>
<td>Shows if the authentication was successful or a failure. This column is required and cannot be deselected. Green is used to represent passed authentications. Red is used to represent failed authentications.</td>
</tr>
<tr>
<td>Details</td>
<td>Brings up a report when you click the magnifying glass icon, allowing you to drill down and view more detailed information on the selected authentication scenario. This column is required and cannot be deselected.</td>
</tr>
<tr>
<td>Session Key</td>
<td>Shows the session keys (found in the EAP success or EAP failure messages) returned by ISE to the network device.</td>
</tr>
<tr>
<td>Username</td>
<td>Shows the user name of the device administrator. This column is required and cannot be deselected.</td>
</tr>
<tr>
<td>Type</td>
<td>Consists of two Types—Authentication and Authorization. Shows user names who have passed or failed authentication, authorization, or both. This column is required and cannot be deselected.</td>
</tr>
<tr>
<td>Authentication Policy</td>
<td>Shows the name of the policy selected for specific authentication.</td>
</tr>
<tr>
<td>Authorization Policy</td>
<td>Shows the name of the policy selected for specific authorization.</td>
</tr>
<tr>
<td>ISE Node</td>
<td>Shows the name of the ISE Node through which the access request is processed.</td>
</tr>
<tr>
<td>Network Device Name</td>
<td>Shows the names of network devices.</td>
</tr>
<tr>
<td>Network Device IP</td>
<td>Shows the IP addresses of network devices whose access requests are processed.</td>
</tr>
<tr>
<td>Network Device Groups</td>
<td>Shows the name of the corresponding network device group to which a network device belongs.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Shows the device type policy used to process access requests from different network devices.</td>
</tr>
</tbody>
</table>
### Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Shows the location based policy used to process access requests from network devices.</td>
</tr>
<tr>
<td>Device Port</td>
<td>Shows the device port number through which the access request is made.</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>Shows the reason for rejecting an access request made by a network device.</td>
</tr>
<tr>
<td>Remote Address</td>
<td>Shows the IP address, MAC address, or any other string that uniquely identifies the end station.</td>
</tr>
<tr>
<td>Matched Command Set</td>
<td>Shows the MatchedCommandSet attribute value if it is present or shows an empty value if the MatchedCommandSet attribute value is empty or attribute itself does not exist in the syslog.</td>
</tr>
<tr>
<td>Shell Profile</td>
<td>Shows the privileges that were granted to a device administrator for executing commands on the network device.</td>
</tr>
</tbody>
</table>

You can do the following in the TACACS Live Logs page:

- Export the data in csv or pdf format.
- Show or hide the columns based on your requirements.
- Filter the data using quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
- Sort the column values.

---

**Note**

All the user customizations will be stored as user preferences.

**Related Topics**

- [TACACS+ Device Administration](#), on page 7
- [Configure Global TACACS+ Settings](#), on page 208

---

**Diagnostic Tools**

### RADIUS Authentication Troubleshooting Settings

The following table describes the fields on the RADIUS authentication troubleshooting page which allow you to identify and resolve RADIUS authentication problems. The navigation path for this page is: **Operations > Troubleshoot > Diagnostic Tools > General Tools > RADIUS Authentication Troubleshooting.**
Table 170: RADIUS Authentication Troubleshooting Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter the username of the user whose authentication you want to troubleshoot.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Enter the MAC address of the device that you want to troubleshoot.</td>
</tr>
<tr>
<td>Audit Session ID</td>
<td>Enter the audit session ID that you want to troubleshoot.</td>
</tr>
<tr>
<td>NAS IP</td>
<td>Enter the NAS IP address.</td>
</tr>
<tr>
<td>NAS Port</td>
<td>Enter the NAS port number.</td>
</tr>
<tr>
<td>Authentication Status</td>
<td>Choose the status of your RADIUS authentication.</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>Enter the failure reason or click <strong>Select</strong> to choose a failure reason from a list. Click <strong>Clear</strong> to clear the failure reason.</td>
</tr>
<tr>
<td>Time Range</td>
<td>Select a time range. The RADIUS authentication records that are created during this time range are used.</td>
</tr>
<tr>
<td>Start Date-Time</td>
<td>If you choose Custom Time Range, enter the start date and time, or click the calendar icon to select the start date and time. The date should be in the <em>mm/dd/yyyy</em> format and time in the <em>hh:mm</em> format.</td>
</tr>
<tr>
<td>End Date-Time</td>
<td>If you choose Custom Time Range, enter the end date and time, or click the calendar icon to select the end date and time. The date should be in the <em>mm/dd/yyyy</em> format and time in the <em>hh:mm</em> format.</td>
</tr>
<tr>
<td>Fetch Number of Records</td>
<td>Choose the number of records that you want to fetch from the drop-down list: 10, 20, 50, 100, 200, or 500.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Troubleshoot Unexpected RADIUS Authentication Results, on page 887
- RADIUS Authentication Troubleshooting Tool, on page 887

**Execute Network Device Command Settings**

The following table describes the fields on the Execute Network Device Command page, which you use to execute the **show** command on a network device. The navigation path for this page is: **Operations > Troubleshoot > Diagnostic Tools > General Tools > Execute Network Device.**
Table 171: Execute Network Device Command Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Information</td>
<td></td>
</tr>
<tr>
<td>Network Device IP</td>
<td>Enter the IP address of the network device on which you want to run the command.</td>
</tr>
<tr>
<td>Command</td>
<td>Enter the <code>show</code> command.</td>
</tr>
</tbody>
</table>

Related Topics
- Execute IOS Show Commands to Check Configuration, on page 888
- Execute Network Device Tool, on page 888

Evaluate Configuration Validator Settings

The following table describes the fields on the Evaluate Configuration Validator page, which you use to evaluate the configuration of a network device and identify any configuration problems. The navigation path for this page is: Operations > Troubleshoot > Diagnostic Tools > General Tools > Evaluate Configuration Validator.

Table 172: Evaluate Configuration Validator Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Information</td>
<td></td>
</tr>
<tr>
<td>Network Device IP</td>
<td>Enter the IP address of the network device whose configuration you want to evaluate.</td>
</tr>
<tr>
<td>Select the configuration items below that you want to compare against the recommended template.</td>
<td></td>
</tr>
<tr>
<td>AAA</td>
<td>This option is selected by default.</td>
</tr>
<tr>
<td>RADIUS</td>
<td>This option is selected by default.</td>
</tr>
<tr>
<td>Device Discovery</td>
<td>This option is selected by default.</td>
</tr>
<tr>
<td>Logging</td>
<td>This option is selected by default.</td>
</tr>
<tr>
<td>Web Authentication</td>
<td>Check this check box to compare the web authentication configuration.</td>
</tr>
<tr>
<td>Profiler Configuration</td>
<td>Check this check box to compare the Profiler configuration.</td>
</tr>
<tr>
<td>Trustsec</td>
<td>Check this check box if you want to compare Trustsec configuration.</td>
</tr>
<tr>
<td>802.1X</td>
<td>Check this check box if you want to compare the 802.1X configuration, and choose one of the available options.</td>
</tr>
</tbody>
</table>
Posture Troubleshooting Settings

The following table describes the fields on the Posture troubleshooting page, which you use to find and resolve posture problems on the network. The navigation path for this page is: Operations > Troubleshoot > Diagnostic Tools > General Tools > Posture Troubleshooting.

Table 173: Posture Troubleshooting Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search and Select a Posture event for troubleshooting</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username to filter on.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Enter the MAC address to filter on, using format: xx-xx-xx-xx-xx</td>
</tr>
<tr>
<td>Posture Status</td>
<td>Select the authentication status to filter on:</td>
</tr>
<tr>
<td>Failure Reason</td>
<td>Enter the failure reason or click Select to choose a failure reason from a list. Click Clear to clear the failure reason.</td>
</tr>
<tr>
<td>Time Range</td>
<td>Select a time range. The RADIUS authentication records that are created during this time range are used.</td>
</tr>
<tr>
<td>Start Date-Time:</td>
<td>(Available only when you choose Custom Time Range) Enter the start date and time, or click the calendar icon to select the start date and time. The date should be in the mm/dd/yyyy format and time in the hh:mm format.</td>
</tr>
<tr>
<td>End Date-Time:</td>
<td>(Available only when you choose Custom Time Range) Enter the end date and time, or click the calendar icon to select the start date and time. The date should be in the mm/dd/yyyy format and time in the hh:mm format.</td>
</tr>
<tr>
<td>Fetch Number of Records</td>
<td>Select the number of records to display: 10, 20, 50, 100, 200, 500</td>
</tr>
<tr>
<td>Search Result</td>
<td></td>
</tr>
<tr>
<td>Time</td>
<td>Time of the event</td>
</tr>
<tr>
<td>Status</td>
<td>Posture status</td>
</tr>
<tr>
<td>Username</td>
<td>User name associated with the event</td>
</tr>
</tbody>
</table>
TCP Dump Settings

The following table describes the fields on the tcpdump utility page, which you use to monitor the contents of packets on a network interface and troubleshoot problems on the network as they appear. The navigation path for this page is: Operations > Troubleshoot > Diagnostic Tools > General Tools > TCP Dump.

Table 174: TCP Dump Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>• Stopped—the tcpdump utility is not running</td>
</tr>
<tr>
<td></td>
<td>• Start—Click to start the tcpdump utility monitoring the network.</td>
</tr>
<tr>
<td></td>
<td>• Stop—Click to stop the tcpdump utility</td>
</tr>
<tr>
<td>Host Name</td>
<td>Choose the name of the host to monitor from the drop-down list.</td>
</tr>
<tr>
<td>Network Interface</td>
<td>Choose the network interface to monitor from the drop-down list.</td>
</tr>
<tr>
<td>Note</td>
<td>You must configure all network interface cards (NICs) with an IPv4 or IPv6 address so that they are displayed in the Cisco ISE Admin portal.</td>
</tr>
<tr>
<td>Promiscuous Mode</td>
<td>• On—Click to turn on promiscuous mode (default).</td>
</tr>
<tr>
<td></td>
<td>• Off—Click to turn off promiscuous mode.</td>
</tr>
</tbody>
</table>

Promiscuous mode is the default packet sniffing mode. It is recommended that you leave it set to On. In this mode the network interface is passing all traffic to the system’s CPU.
### SXP-IP Mappings

The following table describes the fields on the SXP-IP mappings page, which you use to compare mappings between a device and its peers. The navigation path for this page is: **Operations > Troubleshoot > Diagnostic Tools > Trustsec Tools > SXP-IP Mappings**.

#### Peer SXP Devices

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer SXP Devices</td>
<td></td>
</tr>
<tr>
<td>Peer IP Address</td>
<td>IP address of the peer SXP device.</td>
</tr>
<tr>
<td>VRF</td>
<td>The VRF instance of the peer device.</td>
</tr>
</tbody>
</table>
### Usage Guidelines

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer SXP Mode</td>
<td>The SXP mode of the peer device; for example, whether it is a speaker or a listener.</td>
</tr>
<tr>
<td>Self SXP Mode</td>
<td>The SXP mode of the network device; for example, whether it is a speaker or a listener.</td>
</tr>
<tr>
<td>Connection State</td>
<td>The status of the connection.</td>
</tr>
</tbody>
</table>

#### Common Connection Parameters

<table>
<thead>
<tr>
<th>User Common Connection Parameters</th>
<th>Check this check box to enable common connection parameters for all the peer SXP devices.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>If the common connection parameters are not specified or if they do not work for some reason, the Expert Troubleshooter again prompts you for connection parameters for that particular peer device.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Username</th>
<th>Enter the username of the peer SXP device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>Enter the password to gain access to the peer device.</td>
</tr>
<tr>
<td>Protocol</td>
<td>• Choose the protocol.</td>
</tr>
<tr>
<td>Note</td>
<td>Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.</td>
</tr>
<tr>
<td>Port</td>
<td>• Enter the port number.</td>
</tr>
<tr>
<td>Note</td>
<td>The default port number for Telnet is 23 and SSH is 22.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Enter the enable password if it is different from your login password.</td>
</tr>
<tr>
<td>Same as login password</td>
<td>Check this check box if your enable password is the same as your login password.</td>
</tr>
</tbody>
</table>

### Related Topics
- Troubleshoot Connectivity Issues in a Trustsec-Enabled Network with SXP-IP Mappings, on page 894
- Support for SXP, on page 7

### IP User SGT

The following table describes the fields on the IP User SGT page, which you use to compare IP-SGT values on a device with an ISE assigned SGT. The navigation path for this page is: **Operations > Troubleshoot > Diagnostic Tools > TrustSec Tools > IP User SGT.**
Table 176: IP User SGT

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Information</td>
<td></td>
</tr>
<tr>
<td>Network Device IP</td>
<td>Enter the IP address of the network device.</td>
</tr>
<tr>
<td>Filter Results</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username of the user whose records you want to troubleshoot.</td>
</tr>
<tr>
<td>User IP Address</td>
<td>Enter the IP address of the user whose records you want to troubleshoot.</td>
</tr>
<tr>
<td>SGT</td>
<td>Enter the user SGT value.</td>
</tr>
</tbody>
</table>

Related Topics

Troubleshoot Connectivity Issues in a Trustsec-Enabled Network with IP-SGT Mappings, on page 894
Security Groups Configuration, on page 818

Device SGT Settings

The following table describes the fields on the Device SGT page, which you use to compare the device SGT with the most recently assigned value. The navigation path for this page is: Operations > Troubleshoot > Diagnostic Tools > Trustsec Tools > Device SGT.

Table 177: Device SGT Settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Information</td>
<td></td>
</tr>
<tr>
<td>Network Device IPs (comma-separated list)</td>
<td>Enter the network device IP addresses (whose device SGT you want to compare with an ISE-assigned device SGT) separated by commas.</td>
</tr>
<tr>
<td>Common Connection Parameters</td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Use Common Connection Parameters</td>
<td>Select this check box to use the following common connection parameters for comparison:</td>
</tr>
<tr>
<td></td>
<td>• Username—Enter the username of the network device.</td>
</tr>
<tr>
<td></td>
<td>• Password—Enter the password.</td>
</tr>
<tr>
<td></td>
<td>• Protocol—Choose the protocol.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Telnet is the default option. If you choose SSHv2, SSH connections must be enabled on the network device.</td>
</tr>
<tr>
<td></td>
<td>• Port—Enter the port number. The default port number for Telnet is 23 and SSH is 22.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Enter the enable password if it is different from your login password.</td>
</tr>
<tr>
<td>Same as login password</td>
<td>Select this check box if your enable password is the same as your login password.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Troubleshoot Connectivity Issues in a Trustsec-Enabled Network by Comparing Device SGT Mappings, on page 895
- Device SGT Tool, on page 895

**Progress Details Settings**

The following table describes the fields on the Progress Details page, which is displayed when you click the User Input Required button in any of the diagnostic tools. This page displays detailed troubleshooting information. The navigation path for this page is: Operations > Troubleshoot > Diagnostic Tools > Any Diagnostic Tool.

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specify Connection Parameters for Network</td>
<td></td>
</tr>
<tr>
<td>Device a.b.c.d</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>Enter the username for logging in to the network device.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password.</td>
</tr>
<tr>
<td>Option</td>
<td>Usage Guidelines</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Protocol</td>
<td>Choose the protocol.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port number.</td>
</tr>
<tr>
<td>Enable Password</td>
<td>Enter the enable password.</td>
</tr>
<tr>
<td>Same As Login Password</td>
<td>Check this check box if the enable password is the same as the login password.</td>
</tr>
<tr>
<td>Use Console Server</td>
<td>Select this check box to use the console server.</td>
</tr>
<tr>
<td>Console IP Address</td>
<td>(If the Use Console Server check box is selected) Enter the console IP address.</td>
</tr>
</tbody>
</table>

**Advanced (Use if there is an “Expect timeout error” or the device has non-standard prompt strings)**

**Note** The Advanced options appear only for some of the troubleshooting tools.

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username Expect String</td>
<td>Enter the string that the network device uses to prompt for username; for example, Username:, Login:, and so on.</td>
</tr>
<tr>
<td>Password Expect String</td>
<td>Enter the string that the network device uses to prompt for password; for example, Password:.</td>
</tr>
<tr>
<td>Prompt Expect String</td>
<td>Enter the prompt that the network device uses. For example, #, &gt;, and @.</td>
</tr>
<tr>
<td>Authentication Failure Expect String</td>
<td>Enter the string that the network device returns when there is an authentication failure; for example, Incorrect password, Login invalid, and so on.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Troubleshoot Unexpected RADIUS Authentication Results, on page 887
- Execute IOS Show Commands to Check Configuration, on page 888
- Troubleshoot Network Device Configuration Issues, on page 888
- Troubleshoot Connectivity Issues in a Trustsec-Enabled Network with SXP-IP Mappings, on page 894
- Troubleshoot Connectivity Issues in a Trustsec-Enabled Network with IP-SGT Mappings, on page 894
- Diagnostic Troubleshooting Tools, on page 887

**Results Summary**

The following table describes the fields on the results summary page, which is displayed as a result when you use any diagnostic tool.
Table 179: RADIUS Authentication Troubleshooting Results Summary

<table>
<thead>
<tr>
<th>Option</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diagnosis and Resolution</td>
<td></td>
</tr>
<tr>
<td>Diagnosis</td>
<td>The diagnosis for the problem is listed here.</td>
</tr>
<tr>
<td>Resolution</td>
<td>The steps for resolution of the problem are detailed here.</td>
</tr>
<tr>
<td>Troubleshooting Summary</td>
<td></td>
</tr>
<tr>
<td>Summary</td>
<td>A step-by-step summary of troubleshooting information is provided here. You can expand any step to view further details. Any configuration errors are indicated by red text.</td>
</tr>
</tbody>
</table>

Related Topics

- Troubleshoot Unexpected RADIUS Authentication Results, on page 887
- RADIUS Authentication Troubleshooting Tool, on page 887

Export Summary

You can view the details of the reports exported by all the users in the last 7 days along with the status. The export summary includes both the manual and scheduled reports. The export summary page is automatically refreshed every 2 minutes. Click the Refresh icon to refresh the export summary page manually.

The super admin can cancel the export which is in-progress or in queued state. Other users are allowed only to cancel the export process that they have initiated.

By default, only 3 manual export of reports can run at a given point of time and the remaining triggered manual export of reports will be queued. There are no such limits for the scheduled export of reports.

Note

- All the reports in the queued state will be scheduled again and the reports in the In-Progress or Cancellation-in-progress state will be marked as failed when the Cisco ISE server is restarted.

Note

- If the primary MnT node is down, the scheduled report export job will run on secondary MnT node.

The following table describes the fields in the Export Summary page. The navigation path for this page is: Operations > Reports > Export Summary.

Table 180: Export Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Exported</td>
<td>Displays the name of the report.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Exported By</td>
<td>Shows the role of the user who initiated the export process.</td>
</tr>
<tr>
<td>Scheduled</td>
<td>Shows whether the report export is a scheduled one.</td>
</tr>
<tr>
<td>Triggered On</td>
<td>Shows the time when the export process has been triggered in the system.</td>
</tr>
<tr>
<td>Repository</td>
<td>Displays the name of the repository where the exported data will be stored.</td>
</tr>
<tr>
<td>Filter Parameters</td>
<td>Shows the filter parameters selected while exporting the report.</td>
</tr>
<tr>
<td>Status</td>
<td>Shows the status of the exported reports. It can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Queued</td>
</tr>
<tr>
<td></td>
<td>• In-progress</td>
</tr>
<tr>
<td></td>
<td>• Completed</td>
</tr>
<tr>
<td></td>
<td>• Cancellation-in-progress</td>
</tr>
<tr>
<td></td>
<td>• Cancelled</td>
</tr>
<tr>
<td></td>
<td>• Failed</td>
</tr>
<tr>
<td></td>
<td>• Skipped</td>
</tr>
</tbody>
</table>

**Note**

Failed status indicates the reason for failure. Skipped status indicates that the scheduled export of reports is skipped as the primary MnT node is down.

You can do the following in the Export Summary page:

- Show or hide the columns based on your requirements.
- Filter the data using quick or custom filter. You can also save your filters for later use.
- Rearrange the columns and adjust the width of the columns.
Network Access Flows

- Password-Based Authentication, on page 1173
- RADIUS Protocol Support in Cisco ISE, on page 1174
- Network Access for Users, on page 1174

Password-Based Authentication

Authentication verifies user information to confirm user identity. Traditional authentication uses a name and a fixed password. This is the most popular, simplest, and least-expensive method of authentication. The disadvantage is that this information can be told to someone else, guessed, or captured. An approach that uses simple, unencrypted usernames and passwords is not considered a strong authentication mechanism, but it can be sufficient for low-authorization or low-privilege levels such as Internet access.

Secure Authentication Using Encrypted Passwords and Cryptographic Techniques

You should use encryption to reduce the risk of password capture on the network. Client and server access control protocols, such as RADIUS, encrypt passwords to prevent them from being captured within a network. However, RADIUS operates only between the authentication, authorization, and accounting (AAA) client and Cisco ISE. Before this point in the authentication process, unauthorized persons can obtain cleartext passwords such as in the following examples:

- In the communication between an end-user client that dials up over a phone line
- On an ISDN line that terminates at a network access server
- Over a Telnet session between an end-user client and the hosting device

More-secure methods use cryptographic techniques, such as those used inside the Challenge Authentication Handshake Protocol (CHAP), one-time password (OTP), and advanced EAP-based protocols. Cisco ISE supports a variety of these authentication methods.
Authentication Methods and Authorization Privileges

A fundamental implicit relationship exists between authentication and authorization. The more authorization privileges that are granted to a user, the stronger the authentication should be. Cisco ISE supports this relationship by providing various methods of authentication.

RADIUS Protocol Support in Cisco ISE

RADIUS is a client/server protocol through which remote-access servers communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. You can use RADIUS to maintain user profiles in a central database that all remote servers can share. This protocol provides better security, and you can use it to set up a policy that is applied at a single administered network point.

RADIUS also functions as a RADIUS client in Cisco ISE to proxy requests to a remote RADIUS server, and it provides Change of Authorization (CoA) activities during an active session.

Cisco ISE supports RADIUS protocol flow according to RFC 2865 and generic support for all general RADIUS attributes as described in RFC 2865 and its extension. Cisco ISE supports parsing of vendor-specific attributes only for vendors that are defined in the Cisco ISE dictionary.

RADIUS interface supports the following attribute data types that are defined in RFC 2865:

- Text (Unicode Transformation Format [UTF])
- String (binary)
- Address (IP)
- Integer
- Time

ISE Community Resource

For information about the network access attributes supported by Cisco ISE, see ISE Network Access Attributes.

Network Access for Users

For network access, a host connects to the network device and requests to use network resources. The network device identifies the newly connected host, and, using the RADIUS protocol as a transport mechanism, requests Cisco ISE to authenticate and authorize the user.

Cisco ISE supports network access flows depending on the protocol that is transported over the RADIUS protocol.

RADIUS-Based Protocols Without EAP

RADIUS-based protocols that do not include EAP include the following:

- Password Authentication Protocol (PAP)
- CHAP
- Microsoft Challenge Handshake Authentication Protocol version 1 (MS-CHAPv1)
- MS-CHAP version 2 (MS-CHAPv2)

RADIUS-Based Non-EAP Authentication Flow

This section describes RADIUS-based flow without EAP authentication. RADIUS-based flow with PAP authentication occurs in the following process:

1. A host connects to a network device.
2. The network device sends a RADIUS request (Access-Request) to Cisco ISE that contains RADIUS attributes that are appropriate to the specific protocol that is being used (PAP, CHAP, MS-CHAPv1, or MS-CHAPv2).
3. Cisco ISE uses an identity store to validate user credentials.
4. A RADIUS response (Access-Accept or Access-Reject) is sent to the network device that will apply the decision.

The following figure shows a RADIUS-based authentication without EAP.

Figure 68: RADIUS-Based Authentication Without EAP

The non-EAP protocols supported by Cisco ISE are:

Password Authentication Protocol

PAP provides a simple method for users to establish their identity by using a two-way handshake. The PAP password is encrypted with a shared secret and is the least sophisticated authentication protocol. PAP is not a strong authentication method because it offers little protection from repeated trial-and-error attacks.

RADIUS-Based PAP Authentication in Cisco ISE

Cisco ISE checks the username and password pair against the identity stores, until it eventually acknowledges the authentication or terminates the connection.

You can use different levels of security concurrently with Cisco ISE for different requirements. PAP applies a two-way handshaking procedure. If authentication succeeds, Cisco ISE returns an acknowledgment; otherwise, Cisco ISE terminates the connection or gives the originator another chance.

The originator is in total control of the frequency and timing of the attempts. Therefore, any server that can use a stronger authentication method will offer to negotiate that method prior to PAP. RFC 1334 defines PAP.
Cisco ISE supports standard RADIUS PAP authentication that is based on the RADIUS UserPassword attribute. RADIUS PAP authentication is compatible with all identity stores. The RADIUS-with-PAP-authentication flow includes logging of passed and failed attempts.

**Challenge Handshake Authentication Protocol**

CHAP uses a challenge-response mechanism with one-way encryption on the response. CHAP enables Cisco ISE to negotiate downward from the most-secure to the least-secure encryption mechanism, and it protects passwords that are transmitted in the process. CHAP passwords are reusable. If you are using the Cisco ISE internal database for authentication, you can use PAP or CHAP. CHAP does not work with the Microsoft user database. Compared to RADIUS PAP, CHAP allows a higher level of security for encrypting passwords when communicating from an end-user client to the AAA client.

Cisco ISE supports standard RADIUS CHAP authentication that is based on the RADIUS ChapPassword attribute. Cisco ISE supports RADIUS CHAP authentication only with internal identity stores.

**Microsoft Challenge Handshake Authentication Protocol Version 1**

Cisco ISE supports the RADIUS MS-CHAPv1 authentication and change-password features. RADIUS MS-CHAPv1 contains two versions of the change-password feature: Change-Password-V1 and Change-Password-V2. Cisco ISE does not support Change-Password-V1 based on the RADIUS MS-CHAP-CPW-1 attribute, and supports only Change-Password-V2 based on the MS-CHAP-CPW-2 attribute. The RADIUS MS-CHAPv1 authentication and change-password features are supported with the following identity sources:

- Internal identity stores
- Microsoft Active Directory identity store

**Microsoft Challenge Handshake Authentication Protocol Version 2**

The RADIUS MS-CHAPv2 authentication and change-password features are supported with the following identity sources:

- Internal identity stores
- Microsoft Active Directory identity store

**RADIUS-Based EAP Protocols**

EAP provides an extensible framework that supports various authentication types. This section describes the EAP methods supported by Cisco ISE and contains the following topics:

### Simple EAP Methods

- EAP-Message Digest 5
- Lightweight EAP

### EAP Methods That Use Cisco ISE Server Certificate for Authentication

- PEAP/EAP-MS-CHAPv2
Apart from the methods listed above, there are EAP methods that use certificates for both server and client authentication.

RADIUS-Based EAP Authentication Flow

Whenever EAP is involved in the authentication process, the process is preceded by an EAP negotiation phase to determine which specific EAP method (and inner method, if applicable) should be used. EAP-based authentication occurs in the following process:

1. A host connects to a network device.
2. The network device sends an EAP Request to the host.
3. The host replies with an EAP Response to the network device.
4. The network device encapsulates the EAP Response that it received from the host into a RADIUS Access-Request (using the EAP-Message RADIUS attribute) and sends the RADIUS Access-Request to Cisco ISE.
5. Cisco ISE extracts the EAP Response from the RADIUS packet and creates a new EAP Request, encapsulates it into a RADIUS Access-Challenge (again, using the EAP-Message RADIUS attribute), and sends it to the network device.
6. The network device extracts the EAP Request and sends it to the host.

In this way, the host and Cisco ISE indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication.

The EAP messages that are subsequently exchanged are then used to carry the data that is needed to perform the actual authentication. If it is required by the specific EAP authentication method that is negotiated, Cisco ISE uses an identity store to validate user credentials.

After Cisco ISE determines whether the authentication should pass or fail, it sends either an EAP-Success or EAP-Failure message, encapsulated into a RADIUS Access-Accept or Access-Reject message to the network device (and ultimately also to the host).

The following figure shows a RADIUS-based authentication with EAP.

*Figure 69: RADIUS-Based Authentication with EAP*
Extensible Authentication Protocol-Message Digest 5

Extensible Authentication Protocol-Message Digest 5 (EAP-MD5) provides one-way client authentication. The server sends the client a random challenge. The client proves its identity in a response by encrypting the challenge and its password with MD5. Because a man in the middle could see the challenge and response, EAP-MD5 is vulnerable to dictionary attack when used over an open medium. Because no server authentication occurs, it is also vulnerable to spoofing. Cisco ISE supports EAP-MD5 authentication against the Cisco ISE internal identity store. Host Lookup is also supported when using the EAP-MD5 protocol.

Lightweight Extensible Authentication Protocol

Cisco ISE currently uses Lightweight Extensible Authentication Protocol (LEAP) only for Cisco Aironet wireless networking. If you do not enable this option, Cisco Aironet end-user clients who are configured to perform LEAP authentication cannot access the network. If all Cisco Aironet end-user clients use a different authentication protocol, such as Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), we recommend that you disable this option.

Note

If users access your network by using a AAA client that is defined in the Network Devices section as a RADIUS (Cisco Aironet) device, then you must enable LEAP, EAP-TLS, or both; otherwise, Cisco Aironet users cannot authenticate.

Protected Extensible Authentication Protocol

Protected Extensible Authentication Protocol (PEAP) provides mutual authentication, ensures confidentiality and integrity to vulnerable user credentials, protects itself against passive (eavesdropping) and active (man-in-the-middle) attacks, and securely generates cryptographic keying material. PEAP is compatible with the IEEE 802.1X standard and RADIUS protocol. Cisco ISE supports PEAP version 0 (PEAPv0) and PEAP version 1 (PEAPv1) with Extensible Authentication Protocol-Microsoft Challenge Handshake Authentication Protocol (EAP-MS-CHAP), Extensible Authentication Protocol-Generic Token Card (EAP-GTC), and EAP-TLS inner methods. The Cisco Secure Services Client (SSC) supplicant supports all of the PEAPv1 inner methods that Cisco ISE supports.

Advantages of Using PEAP

Using PEAP presents these advantages: PEAP is based on TLS, which is widely implemented and has undergone extensive security review. It establishes a key for methods that do not derive keys. It sends an identity within the tunnel. It protects inner method exchanges and the result message. It supports fragmentation.

Supported Supplicants for the PEAP Protocol

PEAP supports these supplicants:

- Microsoft Built-In Clients 802.1X XP
- Microsoft Built-In Clients 802.1X Vista
- Cisco Secure Services Client (SSC), Release 4.0
- Cisco SSC, Release 5.1
- Funk Odyssey Access Client, Release 4.72
- Intel, Release 12.4.0.0
PEAP Protocol Flow

A PEAP conversation can be divided into three parts:

1. Cisco ISE and the peer build a TLS tunnel. Cisco ISE presents its certificate, but the peer does not. The peer and Cisco ISE create a key to encrypt the data inside the tunnel.

2. The inner method determines the flow within the tunnel:
   - EAP-MS-CHAPv2 inner method—EAP-MS-CHAPv2 packets travel inside the tunnel without their headers. The first byte of the header contains the type field. EAP-MS-CHAPv2 inner methods support the change-password feature. You can configure the number of times that the user can attempt to change the password through the Admin portal. User authentication attempts are limited by this number.
   - EAP-GTC inner method—Both PEAPv0 and PEAPv1 support the EAP-GTC inner method. The supported supplicants do not support PEAPv0 with the EAP-GTC inner method. EAP-GTC supports the change-password feature. You can configure the number of times that the user can attempt to change the password through the Admin portal. User authentication attempts are limited by this number.
   - EAP-TLS inner method—The Windows built-in supplicant does not support fragmentation of messages after the tunnel is established, and this affects the EAP-TLS inner method. Cisco ISE does not support fragmentation of the outer PEAP message after the tunnel is established. During tunnel establishment, fragmentation works as specified in PEAP documentation. In PEAPv0, EAP-TLS packet headers are removed, and in PEAPv1, EAP-TLS packets are transmitted unchanged.
   - Extensible Authentication Protocol-type, length, value (EAP-TLV) extension—EAP-TLV packets are transmitted unchanged. EAP-TLV packets travel with their headers inside the tunnel.

3. There is protected acknowledgment of success and failure if the conversation has reached the inner method.

   The client EAP message is always carried in the RADIUS Access-Request message, and the server EAP message is always carried in the RADIUS Access-Challenge message. The EAP-Success message is always carried in the RADIUS Access-Accept message. The EAP-Failure message is always carried in the RADIUS Access-Reject message. Dropping the client PEAP message results in dropping the RADIUS client message.

Note: Cisco ISE requires acknowledgment of the EAP-Success or EAP-Failure message during PEAPv1 communication. The peer must send back a PEAP packet with empty TLS data field to acknowledge the receipt of success or failure message.

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST) is an authentication protocol that provides mutual authentication and uses a shared secret to establish a tunnel. The tunnel is used to protect weak authentication methods that are based on passwords. The shared secret, referred to as a Protected Access Credentials (PAC) key, is used to mutually authenticate the client and server while securing the tunnel.
Benefits of EAP-FAST

EAP-FAST provides the following benefits over other authentication protocols:

- **Mutual authentication**—The EAP server must be able to verify the identity and authenticity of the peer, and the peer must be able to verify the authenticity of the EAP server.
- **Immunity to passive dictionary attacks**—Many authentication protocols require a password to be explicitly provided, either as cleartext or hashed, by the peer to the EAP server.
- **Immunity to man-in-the-middle attacks**—In establishing a mutually authenticated protected tunnel, the protocol must prevent adversaries from successfully interjecting information into the conversation between the peer and the EAP server.
- **Flexibility to enable support for many different password authentication interfaces such as MS-CHAPv2, Generic Token Card (GTC), and others**—EAP-FAST is an extensible framework that allows support of multiple internal protocols by the same server.
- **Efficiency**—When using wireless media, peers are limited in computational and power resources. EAP-FAST enables the network access communication to be computationally lightweight.
- **Minimization of the per-user authentication state requirements of the authentication server**—With large deployments, it is typical to have many servers acting as the authentication servers for many peers. It is also highly desirable for a peer to use the same shared secret to secure a tunnel much the same way that it uses the username and password to gain access to the network. EAP-FAST facilitates the use of a single, strong, shared secret by the peer, while enabling servers to minimize the per-user and device state that it must cache and manage.

EAP-FAST Flow

The EAP-FAST protocol flow is always a combination of the following phases:

1. **Provisioning phase**—This is phase zero of EAP-FAST. During this phase, the peer is provisioned with a unique, strong secret that is referred to as the PAC that is shared between the Cisco ISE and the peer.
2. **Tunnel establishment phase**—The client and server authenticate each other by using the PAC to establish a fresh tunnel key. The tunnel key is then used to protect the rest of the conversation and provides message confidentiality and with authenticity.
3. **Authentication phase**—The authentication is processed inside the tunnel and includes the generation of session keys and protected termination. Cisco ISE supports EAP-FAST versions 1 and 1a.
Switch and Wireless LAN Controller Configuration Required to Support Cisco ISE Functions

To ensure Cisco ISE is able to interoperate with network switches and functions from Cisco ISE are successful across the network segment, you need to configure network switches with the necessary NTP, RADIUS/AAA, 802.1X, MAB, and other settings for communication with Cisco ISE.

- Enable Your Switch to Support Standard Web Authentication, on page 1181
- Local Username and Password Definition for Synthetic RADIUS Transactions, on page 1182
- NTP Server Configuration to Ensure Accurate Log and Accounting Timestamps, on page 1182
- Command to Enable AAA Functions, on page 1182
- RADIUS Server Configuration on the Switch, on page 1183
- Command to Enable RADIUS Change of Authorization (CoA), on page 1184
- Command to Enable Device Tracking and DHCP Snooping, on page 1184
- Command to Enable 802.1X Port-Based Authentication, on page 1185
- Command to Enable EAP for Critical Authentications, on page 1185
- Command to Throttle AAA Requests Using Recovery Delay, on page 1185
- VLAN Definitions Based on Enforcement States, on page 1185
- Local (Default) ACLs Definition on the Switch, on page 1186
- Enable Switch Ports for 802.1X and MAB, on page 1188
- Command to Enable EPM Logging, on page 1189
- Command to Enable SNMP Traps, on page 1189
- Command to Enable SNMP v3 Query for Profiling, on page 1190
- Command to Enable MAC Notification Traps for Profiler to Collect, on page 1190
- RADIUS Idle-Timeout Configuration on the Switch, on page 1190
- Wireless LAN Controller Configuration for iOS Supplicant Provisioning, on page 1191
- Configuring ACLs on the Wireless LAN Controller for MDM Interoperability, on page 1191

Enable Your Switch to Support Standard Web Authentication

Ensure that you include the following commands in your switch configuration to enable standard Web Authenticating functions for Cisco ISE, including provisions for URL redirection upon authentication:
ip classless

ip route 0.0.0.0 0.0.0.0 10.1.2.3

ip http server
! Must enable HTTP/HTTPS for URL-redirection on port 80/443

ip http secure-server

Local Username and Password Definition for Synthetic RADIUS Transactions

Enter the following command to enable the switch to talk to the Cisco ISE node as though it is the RADIUS server for this network segment:

username test-radius password 0 abcde123

NTP Server Configuration to Ensure Accurate Log and Accounting Timestamps

Ensure that you specify the same NTP server as you have set in Cisco ISE at Administration > System > Settings > System Time by entering the following command:

ntp server <IP_address>|<domain_name>

Command to Enable AAA Functions

Enter the following commands to enable the various AAA functions between the switch and Cisco ISE, including 802.1X and MAB authentication functions:

aaa new-model
! Creates an 802.1X port-based authentication method list

aaa authentication dot1x default group radius
! Required for VLAN/ACL assignment

aaa authorization network default group radius
! Authentication & authorization for webauth transactions

aaa authorization auth-proxy default group radius
! Enables accounting for 802.1X and MAB authentications
aaa accounting dot1x default start-stop group radius
!

aaa session-id common
!

aaa accounting update periodic 5

! Update AAA accounting information periodically every 5 minutes

aaa accounting system default start-stop group radius
!

aaa server radius dynamic-author <cr>

client 10.0.56.17 server-key cisco

! Enables Cisco ISE to act as a AAA server when interacting with the client at IP address 10.0.56.17

RADIUS Server Configuration on the Switch

Configure the switch to interoperate with Cisco ISE acting as the RADIUS source server by entering the following commands:
!
radius-server attribute 6 on-for-login-auth

! Include RADIUS attribute 8 in every Access-Request

radius-server attribute 8 include-in-access-req

! Include RADIUS attribute 25 in every Access-Request

radius-server attribute 25 access-request include

! Wait 3 x 30 seconds before marking RADIUS server as dead

radius-server dead-criteria time 30 tries 3

! Use RFC-standard ports (1812/1813)
radius-server host <Cisco_ISE_IP_address> auth-port 1812 acct-port 1813 test

username test-radius key 0 <RADIUS-KEY>

!

radius-server vsa send accounting
!

radius-server vsa send authentication
!

! send RADIUS requests from the MANAGEMENT VLAN
We recommend that you configure a dead-criteria time of 30 seconds with 3 retries to provide longer response times for RADIUS requests that use Active Directory for authentication.

Command to Enable RADIUS Change of Authorization (CoA)

Specify the settings to ensure the switch is able to appropriately handle RADIUS Change of Authorization behavior supporting Posture functions from Cisco ISE by entering the following commands:

```
aaa server radius dynamic-author
```

```
client <ISE-IP> server-key 0 abcde123
```

Note

Cisco ISE uses port 1700 (Cisco IOS software default) versus RFC default port 3799 for CoA. Existing Cisco Secure ACS 5.x customers may already have this set to port 3799 if they are using CoA as part of an existing ACS implementation.

Command to Enable Device Tracking and DHCP Snooping

To help provide optional security-oriented functions from Cisco ISE, you can enable device tracking and DHCP snooping for IP substitution in dynamic ACLs on switch ports by entering the following commands:

```
! Optional
ip dhcp snooping
! Required!
ip device tracking
```

In RADIUS Accounting, the DHCP attributes are not sent by IOS sensor to Cisco ISE even when dhcp snooping is enabled. In such cases, the dhcp snooping should be enabled on the VLAN to make the DHCP active.

Use the following commands to enable dhcp snooping on VLAN:

```
ip dhcp snooping
```

```
ip dhcp snooping vlan 1-100
```

(VLAN range should include used for data and vlan)
Command to Enable 802.1X Port-Based Authentication

Enter the following commands to turn 802.1X authentication on for switch ports, globally:

```
dot1x system-auth-control
```

Command to Enable EAP for Critical Authentications

To support supplicant authentication requests over the LAN, enable EAP for critical authentications (Inaccessible Authentication Bypass) by entering the following command:

```
dot1x critical eapol
```

Command to Throttle AAA Requests Using Recovery Delay

When a critical authentication recovery event takes place, you can configure the switch to automatically introduce a delay (in seconds) to ensure Cisco ISE is able to launch services again following recovery by entering the following command:

```
authentication critical recovery delay 1000
```

VLAN Definitions Based on Enforcement States

Enter the following commands to define the VLAN names, numbers, and SVIs based on known enforcement states in your network. Create the respective VLAN interfaces to enable routing between networks. This can be especially helpful to handle multiple sources of traffic passing over the same network segments—traffic from both PCs and the IP phone through which the PC is connected to the network, for example.

```
vlan <VLAN_number>
name ACCESS!

vlan <VLAN_number>
name VOICE
!
interface <VLAN_number>
description ACCESS

ip address 10.1.2.3 255.255.255.0
ip helper-address <DHCP_Server_IP_address>
```
ip helper-address <Cisco_ISE_IP_address>
!

interface <VLAN_number>

description VOICE

ip address 10.2.3.4 255.255.255.0

ip helper-address <DHCP_Server_IP_address>

Local (Default) ACLs Definition on the Switch

Enable these functions on older switches (with Cisco IOS software releases earlier than 12.2(55)SE) to ensure Cisco ISE is able to perform the dynamic ACL updates required for authentication and authorization by entering the following commands:

ip access-list extended ACL-ALLOW

    permit ip any any

!

ip access-list extended ACL-DEFAULT

    remark DHCP

    permit udp any eq bootpc any eq bootps

    remark DNS

    permit udp any any eq domain

    remark Ping

    permit icmp any any

    remark Ping

    permit icmp any any

    remark PXE / TFTP

    permit udp any any eq tftp

    remark Allow HTTP/S to ISE and WebAuth portal
permit tcp any host <Cisco_ISE_IP_address> eq www
permit tcp any host <Cisco_ISE_IP_address> eq 443
permit tcp any host <Cisco_ISE_IP_address> eq 8443
permit tcp any host <Cisco_ISE_IP_address> eq 8905
permit udp any host <Cisco_ISE_IP_address> eq 8905
permit udp any host <Cisco_ISE_IP_address> eq 8906
permit tcp any host <Cisco_ISE_IP_address> eq 8080
permit udp any host <Cisco_ISE_IP_address> eq 9996
remark Drop all the rest
deny ip any any log
!
! The ACL to allow URL-redirection for WebAuth
ip access-list extended ACL~WEBAUTH~REDIRECT
permit tcp any any eq www
permit tcp any any eq 443

---

Note
This configuration on the WLC may increase CPU utilization and raises the risk of system instability. This is an IOS issue and does not adversely affect Cisco ISE.
Enable Switch Ports for 802.1X and MAB

To enable switch ports for 802.1X and MAB:

**Step 1** Enter configuration mode for all of the access switch ports:
```
interface range FastEthernet0/1-8
```

**Step 2** Enable the switch ports for access mode (instead of trunk mode):
```
switchport mode access
```

**Step 3** Statically configure the access VLAN. This provides local provisioning the access VLANs and is required for open-mode authentication:
```
switchport access <VLAN_number>
```

**Step 4** Statically configure the voice VLAN:
```
switchport voice <VLAN_number>
```

**Step 5** Enable open-mode authentication. Open-mode allows traffic to be bridged onto the data and voice VLANs before authentication is completed. We strongly recommend using a port-based ACL in a production environment to prevent unauthorized access.

! Enables pre-auth access before AAA response; subject to port ACL authentication open

**Step 6** Apply a port-based ACL to determine which traffic should be bridged by default from unauthenticated endpoints onto the access VLAN. Because you should allow all access first and enforce policy later, you should apply ACL-ALLOW to permit all traffic through the switch port. You have already created a default ISE authorization to allow all traffic for now because we want complete visibility and do not want to impact the existing end-user experience yet.

! An ACL must be configured to prepend dACLs from AAA server.
```
ip access-group ACL-ALLOW in
```

**Note** Prior to Cisco IOS software Release 12.2(55)SE on DSBU switches, a port ACL is required for dynamic ACLs from a RADIUS AAA server to be applied. Failure to have a default ACL will result in assigned dACLs being ignored by the switch. With Cisco IOS software Release12.2(55)SE, a default ACL will be automatically generated and applied.

**Note** We are using ACL-ALLOW at this point in the lab because we want to enable 802.1X port-based authentication, but without any impact to the existing network. In a later exercise, we will apply a different ACL-DEFAULT, which blocks undesired traffic for a production environment.

**Step 7** Enable Multi-Auth host mode. Multi-Auth is essentially a superset of Multi-Domain Authentication (MDA). MDA only allows a single endpoint in the data domain. When multi-auth is configured, a single authenticated phone is allowed in the voice domain (as with MDA) but an unlimited number of data devices can be authenticated in the data domain.

! Allow voice + multiple endpoints on same physical access port
```
authentication host-mode multi-auth
```

**Note** Multiple data devices (whether virtualized devices or physical devices connected to a hub) behind an IP phone can exacerbate the access ports’ physical link-state awareness.

**Step 8** Enable various authentication method options:
! Enable re-authentication
authenticator periodic
! Enable re-authentication via RADIUS Session-Timeout
authentication timer reauthenticate server
authentication event fail action next-method
authentication event server dead action reinitialize <VLAN_number>
authentication event server alive action reinitialize
! IOS Flex-Auth authentication should do 802.1X then MAB
authentication order dot1x mab
authentication priority dot1x mab
Step 9 Enable 802.1X port control on the switchport:
! Enables port-based authentication on the interface
authentication port-control auto
authentication violation restrict
Step 10 Enable MAC Authentication Bypass (MAB):
! Enable MAC Authentication Bypass (MAB)
mab
Step 11 Enable 802.1X on the switchport
! Enables 802.1X authentication on the interface
dot1x pae authenticator
Step 12 Set the retransmit period to 10 seconds:
dot1x timeout tx-period 10
Note The dot1x tx-period timeout should be set to 10 seconds. Do not change this unless you understand the implications.
Step 13 Enable the portfast feature:
spanning-tree portfast

Command to Enable EPM Logging

Set up standard logging functions on the switch to support possible troubleshooting/recording for Cisco ISE functions:
epm logging

Command to Enable SNMP Traps

Ensure the switch is able to receive SNMP trap transmissions from Cisco ISE over the appropriate VLAN in this network segment:
Command to Enable SNMP v3 Query for Profiling

Configure the switch to ensure SNMP v3 polling takes place as intended to support Cisco ISE profiling services. First, configure the SNMP settings in Cisco ISE by choosing Administration > Network Resources > Network Devices > Add | Edit > SNMP Settings.

```
Snmp-server user <name> <group> v3 auth md5 <string> priv des <string>
```

```
snmp-server group <group> v3 priv
```

```
snmp-server group <group> v3 priv context vlan-1
```

**Note**

The `snmp-server group <group> v3 priv context vlan-1` command must be configured for each context. The `snmp show context` command lists all the context information.

If the SNMP Request times out and there is no connectivity issue, then you can increase the Timeout value.

Command to Enable MAC Notification Traps for Profiler to Collect

Configure your switch to transmit the appropriate MAC notification traps so that the Cisco ISE Profiler function is able to collect information on network endpoints:

```
mac address-table notification change
```

```
mac address-table notification mac-move
```

```
snmp trap mac-notification change added
```

```
snmp trap mac-notification change removed
```

RADIUS Idle-Timeout Configuration on the Switch

To configure the RADIUS Idle-timeout on a switch, use the following command:

```
Switch(config-if)# authentication timer inactivity
```
where inactivity is interval of inactivity in seconds, after which client activity is considered unauthorized.

In Cisco ISE, you can enable this option for any Authorization Policies to which such a session inactivity timer should apply from Policy > Policy Elements > Results > Authorization > Authorization Profiles.

Wireless LAN Controller Configuration for iOS Supplicant Provisioning

For Single SSID

To support Apple iOS-based devices (iPhone/iPad) switching from one SSID to another on the same wireless access point, configure the Wireless LAN Controller (WLC) to enable the “FAST SSID change” function. This function helps ensure iOS-based devices are able to more quickly switch between SSIDs.

For Dual SSID BYOD

Fast SSID must be enabled to support dual SSID BYOD. When Fast SSID changing is enabled, the wireless controller allows clients to move faster between SSIDs. When fast SSID is enabled, the client entry is not cleared and the delay is not enforced. For more information about configuring Fast SSID on a Cisco WLC, see the Cisco Wireless Controller Configuration Guide.

Example WLC Configuration

WLC (config)# FAST SSID change

You might see the following error message while trying to connect to a wireless network for some of the Apple iOS-based devices:

Could not scan for Wireless Networks.

You can ignore this error message because this does not affect the authentication of the device.

Configuring ACLs on the Wireless LAN Controller for MDM Interoperability

You must configure ACLs on the wireless LAN controller for use in authorization policy to redirect nonregistered devices and certificate provisioning. Your ACLs should be in the following sequence.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Allow all outbound traffic from server to client.</td>
</tr>
<tr>
<td>2</td>
<td>(Optional) Allow ICMP inbound traffic from client to server for troubleshooting.</td>
</tr>
<tr>
<td>3</td>
<td>Allow access to MDM server for unregistered and noncompliant devices to download the MDM agent and proceed with compliance checks.</td>
</tr>
<tr>
<td>4</td>
<td>Allow all inbound traffic from client to server to ISE for Web Portal and supplicant, and certificate provisioning flows.</td>
</tr>
<tr>
<td>5</td>
<td>Allow inbound DNS traffic from client to server for name resolution.</td>
</tr>
<tr>
<td>6</td>
<td>Allow inbound DHCP traffic from client to server for IP addresses.</td>
</tr>
<tr>
<td>7</td>
<td>Deny all inbound traffic from client to server to corporate resources for redirection to ISE (as per your company policy).</td>
</tr>
</tbody>
</table>
Step 8  
(Optional) Permit the rest of the traffic.

Example

The following example shows the ACLs for redirecting a nonregistered device to the BYOD flow. In this example, the Cisco ISE ip address is 10.35.50.165, the internal corporate network ip address is 192.168.0.0 and 172.16.0.0 (to redirect), and the MDM server subnet is 204.8.168.0.

*Figure 70: ACLs for Redirecting Nonregistered Device*
CHAPTER 37

Supported Management Information Bases for Cisco ISE Endpoint Profiler

- IF-MIB, on page 1193
- SNMPv2-MIB, on page 1194
- IP-MIB, on page 1194
- CISCO-CDP-MIB, on page 1194
- CISCO-VTP-MIB, on page 1196
- CISCO-STACK-MIB, on page 1196
- BRIDGE-MIB, on page 1196
- OLD-CISCO-INTERFACE-MIB, on page 1196
- CISCO-LWAPP-AP-MIB, on page 1197
- CISCO-LWAPP-DOT11-CLIENT-MIB, on page 1198
- CISCO-AUTH-FRAMEWORK-MIB, on page 1199
- EEE8021-PAE-MIB: RFC IEEE 802.1X, on page 1199
- HOST-RESOURCES-MIB, on page 1200
- LLDP-MIB, on page 1200

**IF-MIB**

**Table 181:**

<table>
<thead>
<tr>
<th>Object</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ifIndex</td>
<td>1.3.6.1.2.1.2.2.1.1</td>
</tr>
<tr>
<td>ifDescr</td>
<td>1.3.6.1.2.1.2.2.1.2</td>
</tr>
<tr>
<td>ifType</td>
<td>1.3.6.1.2.1.2.2.1.3</td>
</tr>
<tr>
<td>ifSpeed</td>
<td>1.3.6.1.2.1.2.2.1.5</td>
</tr>
<tr>
<td>ifPhysAddress</td>
<td>1.3.6.1.2.1.2.2.1.6</td>
</tr>
<tr>
<td>ifAdminStatus</td>
<td>1.3.6.1.2.1.2.2.1.7</td>
</tr>
<tr>
<td>ifOperStatus</td>
<td>1.3.6.1.2.1.2.2.1.8</td>
</tr>
</tbody>
</table>
### SNMPv2-MIB

**Table 182:**

<table>
<thead>
<tr>
<th>Object</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td>sysDescr</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td>sysObjectID</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td>sysUpTime</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td>sysContact</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td>sysName</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td>sysLocation</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td>sysServices</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td>sysORLastChange</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
<tr>
<td>sysORTable</td>
<td>1.3.6.1.2.1.1.1.0</td>
</tr>
</tbody>
</table>

### IP-MIB

**Table 183:**

<table>
<thead>
<tr>
<th>Object</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipAdEntIfIndex</td>
<td>1.3.6.1.2.1.4.20.1.2</td>
</tr>
<tr>
<td>ipAdEntNetMask</td>
<td>1.3.6.1.2.1.4.20.1.3</td>
</tr>
<tr>
<td>ipNetToMediaPhysAddress</td>
<td>1.3.6.1.2.1.4.22.1.2</td>
</tr>
<tr>
<td>ipNetToPhysicalPhysAddress</td>
<td>1.3.6.1.2.1.4.35.1.4</td>
</tr>
</tbody>
</table>

### CISCO-CDP-MIB

**Table 184:**

<table>
<thead>
<tr>
<th>Object</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>cdpCacheEntry</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1</td>
</tr>
<tr>
<td>Object</td>
<td>OID</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>cdpCacheIfIndex</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.1</td>
</tr>
<tr>
<td>cdpCacheDeviceIndex</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.2</td>
</tr>
<tr>
<td>cdpCacheAddressType</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.3</td>
</tr>
<tr>
<td>cdpCacheAddress</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.4</td>
</tr>
<tr>
<td>cdpCacheVersion</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.5</td>
</tr>
<tr>
<td>cdpCacheDeviceId</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.6</td>
</tr>
<tr>
<td>cdpCacheDevicePort</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.7</td>
</tr>
<tr>
<td>cdpCachePlatform</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.8</td>
</tr>
<tr>
<td>cdpCacheCapabilities</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.9</td>
</tr>
<tr>
<td>cdpCacheVTPMgmtDomain</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.10</td>
</tr>
<tr>
<td>cdpCacheNativeVLAN</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.11</td>
</tr>
<tr>
<td>cdpCacheDuplex</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.12</td>
</tr>
<tr>
<td>cdpCacheApplianceID</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.13</td>
</tr>
<tr>
<td>cdpCacheVlanID</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.14</td>
</tr>
<tr>
<td>cdpCachePowerConsumption</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.15</td>
</tr>
<tr>
<td>cdpCacheMTU</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.16</td>
</tr>
<tr>
<td>cdpCacheSysName</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.17</td>
</tr>
<tr>
<td>cdpCacheSysObjectID</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.18</td>
</tr>
<tr>
<td>cdpCachePrimaryMgmtAddrType</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.19</td>
</tr>
<tr>
<td>cdpCachePrimaryMgmtAddr</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.20</td>
</tr>
<tr>
<td>cdpCacheSecondaryMgmtAddrType</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.21</td>
</tr>
<tr>
<td>cdpCacheSecondaryMgmtAddr</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.22</td>
</tr>
<tr>
<td>cdpCachePhysLocation</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.23</td>
</tr>
<tr>
<td>cdpCacheLastChange</td>
<td>1.3.6.1.4.1.9.9.23.1.2.1.1.24</td>
</tr>
</tbody>
</table>
### CISCO-VTP-MIB

**Table 185:**

<table>
<thead>
<tr>
<th>Object</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>vtpVlanIfIndex</td>
<td>1.3.6.1.4.1.9.9.46.1.3.1.1.18.1</td>
</tr>
<tr>
<td>vtpVlanName</td>
<td>1.3.6.1.4.1.9.9.46.1.3.1.1.4.1</td>
</tr>
<tr>
<td>vtpVlanState</td>
<td>1.3.6.1.4.1.9.9.46.1.3.1.1.2.1</td>
</tr>
</tbody>
</table>

### CISCO-STACK-MIB

**Table 186:**

<table>
<thead>
<tr>
<th>Object</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>portIfIndex</td>
<td>1.3.6.1.4.1.9.5.1.4.1.11</td>
</tr>
<tr>
<td>vlanPortVlan</td>
<td>1.3.6.1.4.1.9.5.1.9.3.1.3.1</td>
</tr>
</tbody>
</table>

### BRIDGE-MIB

**Table 187:**

<table>
<thead>
<tr>
<th>Object</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1dTpFdbPort</td>
<td>1.3.6.1.2.1.17.4.3.1.2</td>
</tr>
<tr>
<td>dot1dBasePortIfIndex</td>
<td>1.3.6.1.2.1.17.1.4.1.2</td>
</tr>
</tbody>
</table>

### OLD-CISCO-INTERFACE-MIB

**Table 188:**

<table>
<thead>
<tr>
<th>Object</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>locIfReason</td>
<td>1.3.6.1.4.1.9.2.2.1.1.20</td>
</tr>
</tbody>
</table>
### Table 189:

<table>
<thead>
<tr>
<th>Object</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>cLApEntry</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1</td>
</tr>
<tr>
<td>cLApSysMacAddress</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.1</td>
</tr>
<tr>
<td>cLApIfMacAddress</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.2</td>
</tr>
<tr>
<td>cLApMaxNumberOfDot11Slots</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.3</td>
</tr>
<tr>
<td>cLApEntPhysicalIndex</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.4</td>
</tr>
<tr>
<td>cLApName</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.5</td>
</tr>
<tr>
<td>cLApUpTime</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.6</td>
</tr>
<tr>
<td>cLLwappUpTime</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.7</td>
</tr>
<tr>
<td>cLLwappJoinTakenTime</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.8</td>
</tr>
<tr>
<td>cLApMaxNumberOfEthernetSlots</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.9</td>
</tr>
<tr>
<td>cLApPrimaryControllerAddressType</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.10</td>
</tr>
<tr>
<td>cLApPrimaryControllerAddress</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.11</td>
</tr>
<tr>
<td>cLApSecondaryControllerAddressType</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.1.12</td>
</tr>
<tr>
<td>cLApSecondaryControllerAddress</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.1.13</td>
</tr>
<tr>
<td>cLApTertiaryControllerAddressType</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.1.1.14</td>
</tr>
<tr>
<td>cLApTertiaryControllerAddress</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.1.1.15</td>
</tr>
<tr>
<td>cLApLastRebootReason</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.1.1.16</td>
</tr>
<tr>
<td>cLApEncryptionEnable</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.1.1.17</td>
</tr>
<tr>
<td>cLApFailoverPriority</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.1.1.18</td>
</tr>
<tr>
<td>cLApPowerStatus</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.1.1.1.19</td>
</tr>
<tr>
<td>cLApTelnetEnable</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.1.1.20</td>
</tr>
<tr>
<td>cLApSshEnable</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.1.1.21</td>
</tr>
<tr>
<td>cLApPreStdStateEnabled</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.1.1.1.22</td>
</tr>
<tr>
<td>cLApPwrInjectorStateEnabled</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.1.1.1.23</td>
</tr>
<tr>
<td>cLApPwrInjectorSelection</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.1.1.1.24</td>
</tr>
</tbody>
</table>
### CISCO-LWAPP-DOT11-CLIENT-MIB

#### Table 190:

<table>
<thead>
<tr>
<th>Object</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>cLApPwrInjectorSwMacAddr</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.25</td>
</tr>
<tr>
<td>cLApWipsEnable</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.26</td>
</tr>
<tr>
<td>cLApMonitorModeOptimization</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.27</td>
</tr>
<tr>
<td>cLApDomainName</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.28</td>
</tr>
<tr>
<td>cLApNameServerAddressType</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.29</td>
</tr>
<tr>
<td>cLApNameServerAddress</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.30</td>
</tr>
<tr>
<td>cLApAMSDUEnable</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.31</td>
</tr>
<tr>
<td>cLApEncryptionSupported</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.32</td>
</tr>
<tr>
<td>cLApRogueDetectionEnabled</td>
<td>1.3.6.1.4.1.9.9.513.1.1.1.1.33</td>
</tr>
<tr>
<td>cldcClientEntry</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.1</td>
</tr>
<tr>
<td>cldcClientMacAddress</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.1</td>
</tr>
<tr>
<td>cldcClientStatus</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.2</td>
</tr>
<tr>
<td>cldcClientWlanProfileName</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.3</td>
</tr>
<tr>
<td>cldcClientWgbStatus</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.4</td>
</tr>
<tr>
<td>cldcClientWgbMacAddress</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.5</td>
</tr>
<tr>
<td>cldcClientProtocol</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.6</td>
</tr>
<tr>
<td>cldcAssociationMode</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.7</td>
</tr>
<tr>
<td>cldcApMacAddress</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.8</td>
</tr>
<tr>
<td>cldcIfType</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.9</td>
</tr>
<tr>
<td>cldcClientIPAddress</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.10</td>
</tr>
<tr>
<td>cldcClientNacState</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.11</td>
</tr>
<tr>
<td>cldcClientQuarantineVLAN</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.12</td>
</tr>
<tr>
<td>cldcClientAccessVLAN</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.13</td>
</tr>
</tbody>
</table>
**CISCO-AUTH-FRAMEWORK-MIB**

*Table 191:*

<table>
<thead>
<tr>
<th>Object</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>cldcClientLoginTime</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.14</td>
</tr>
<tr>
<td>cldcClientUpTime</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.15</td>
</tr>
<tr>
<td>cldcClientPowerSaveMode</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.16</td>
</tr>
<tr>
<td>cldcClientCurrentTxRateSet</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.17</td>
</tr>
<tr>
<td>cldcClientDataRateSet</td>
<td>1.3.6.1.4.1.9.9.599.1.3.1.1.18</td>
</tr>
</tbody>
</table>

**EEE8021-PAE-MIB: RFC IEEE 802.1X**

*Table 192:*

<table>
<thead>
<tr>
<th>Object</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1xAuthAuthControlledPortStatus</td>
<td>1.0.8802.1.1.1.1.2.1.1.5</td>
</tr>
<tr>
<td>dot1xAuthAuthControlledPortControl</td>
<td>1.0.8802.1.1.1.1.2.1.1.6</td>
</tr>
<tr>
<td>dot1xAuthSessionUserName</td>
<td>1.0.8802.1.1.1.1.2.4.1.9</td>
</tr>
</tbody>
</table>
### HOST-RESOURCES-MIB

**Table 193:**

<table>
<thead>
<tr>
<th>Object</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>hrDeviceDescr</td>
<td>1.3.6.1.2.1.25.3.2.1.3</td>
</tr>
<tr>
<td>hrDeviceStatus</td>
<td>1.3.6.1.2.1.25.3.2.1.5</td>
</tr>
</tbody>
</table>

### LLDP-MIB

**Table 194:**

<table>
<thead>
<tr>
<th>Object</th>
<th>OID</th>
</tr>
</thead>
<tbody>
<tr>
<td>lldpEntry</td>
<td>1.0.8802.1.1.2.1.4.1.1</td>
</tr>
<tr>
<td>lldpTimeMark</td>
<td>1.0.8802.1.1.2.1.4.1.1.1</td>
</tr>
<tr>
<td>lldpLocalPortNum</td>
<td>1.0.8802.1.1.2.1.4.1.1.2</td>
</tr>
<tr>
<td>lldpIndex</td>
<td>1.0.8802.1.1.2.1.4.1.1.3</td>
</tr>
<tr>
<td>lldpChassisIdSubtype</td>
<td>1.0.8802.1.1.2.1.4.1.1.4</td>
</tr>
<tr>
<td>lldpChassisId</td>
<td>1.0.8802.1.1.2.1.4.1.1.5</td>
</tr>
<tr>
<td>lldpPortIdSubtype</td>
<td>1.0.8802.1.1.2.1.4.1.1.6</td>
</tr>
<tr>
<td>lldpPortId</td>
<td>1.0.8802.1.1.2.1.4.1.1.7</td>
</tr>
<tr>
<td>lldpPortDescription</td>
<td>1.0.8802.1.1.2.1.4.1.1.8</td>
</tr>
<tr>
<td>lldpSystemName</td>
<td>1.0.8802.1.1.2.1.4.1.1.9</td>
</tr>
<tr>
<td>lldpSystemDescription</td>
<td>1.0.8802.1.1.2.1.4.1.1.10</td>
</tr>
<tr>
<td>ldpCapabilitiesMapSupported</td>
<td>1.0.8802.1.1.2.1.4.1.1.11</td>
</tr>
<tr>
<td>lldpCacheCapabilities</td>
<td>1.0.8802.1.1.2.1.4.1.1.12</td>
</tr>
</tbody>
</table>