



Cisco Identity Services Engine Administrator Guide, Release 1.4.1

First Published: April 04, 2016

Last Modified: July 01, 2016

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

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 NON-INFRINGEMENT 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)

© 2016 Cisco Systems, Inc. All rights reserved.



CONTENTS

PART I

Introduction 1

CHAPTER 1

Cisco ISE Features 3

- Cisco ISE Features 4
- Key Functions 4
- Identity-Based Network Access 4
- Support for Multiple Deployment Scenarios 5
- Support for UCS Hardware 5
- Basic User Authentication and Authorization 5
- Policy Sets 6
- FIPS 140-2 Implementation 6
- Support for Common Access Card Functions 7
- Client Posture Assessment 7
- Network Access for Guests 8
- Support for Personal Devices 8
- Mobile Device Manager Interoperability with Cisco ISE 8
- Wireless and VPN Traffic with Inline Posture Nodes 8
- Profiled Endpoints on the Network 9
- Cisco pxGrid Services 9
- Cisco ISE Certificate Authority 9
- Support for Active Directory Multidomain Forests 9
- Support for SAnet Devices 9
- Support for Installation on Multiple Hardware and VMware Platforms 10
- Identity Provider as an External Identity Source 10
- Support for Automatic Failover for the Administration Node 10

CHAPTER 2

Navigate the Admin portal 11

- Admin Portal 12

Cisco ISE Dashboard	13
Setup Assistant	14
Cisco ISE Licensing Impact on Setup Assistant	14
Run the Setup Assistant	14
Setup Assistant Overwrites Previous Configurations	15
Identify Policy Requirements Page in Setup Assistant	15
Configure Network Access Service Page in Setup Assistant	16
Select Network Device Types Page in Setup Assistant	18
Review and Confirm Your Choices Page in Setup Assistant	18
Filter Data on Listing Pages	18
Data Filters in Listing Pages	19
Customize the Displayed Field Attributes	19
Filter Data by Field Attributes Using the Quick Filter	19
Filter Data by Conditions Using the Advanced Filter	20
Create Custom Filters	20
Cisco ISE Internationalization and Localization	20
Supported Languages	20
End-User Web Portal Localization	21
Support for UTF-8 Character Data Entry	22
UTF-8 Credential Authentication	22
UTF-8 Policies and Posture Assessment	22
Cisco NAC and MAC Agent UTF-8 Support	22
UTF-8 Support for Messages Sent to Supplicant	23
Reports and Alerts UTF-8 Support	23
UTF-8 Character Support in the Portals	23
UTF-8 Support Outside the User Interface	26
Support for Importing and Exporting UTF-8 Values	26
UTF-8 Support on REST	26
UTF-8 Support for Identity Stores Authorization Data	27
MAC Address Normalization	27
Admin Features Limited by Role-Based Access Control Policies	27

PART II**Deploy Cisco ISE Nodes 29**

CHAPTER 3**Set Up Cisco ISE in a Distributed Environment 31**

Cisco ISE Distributed Deployment	32
Cisco ISE Deployment Terminology	32
Personas in Distributed Cisco ISE Deployments	32
Administration Node	33
High Availability in Administration Nodes	33
High-Availability Health Check Nodes	35
Health Probe by Health Check Nodes	35
Startup of Health Check Node	35
Shutdown of Health Check Node	36
Restart of Health Check Node	36
Health Check of the Primary Administration Node	36
Automatic Failover of the Secondary Administration Node	36
Sample Scenarios when Automatic Failover is Avoided	37
Fallback to the Original PAN	37
Manual Promotion of the Secondary Administration Node	37
Functionalities Affected by the PAN Auto-Failover Feature	38
Policy Service Node	39
High Availability in Policy Service Nodes	39
Load Balancer To Distribute Requests Evenly Among PSNs	40
Session Failover in Policy Service Nodes	40
Number of Nodes in a Policy Service Node Group	40
Monitoring Node	40
Automatic Failover in Monitoring Nodes	41
Cisco pxGrid Services	42
pxGrid Client and Capability Management	43
Enable pxGrid Clients	43
Cisco pxGrid Live Logs	43
ISE pxGrid Identity Mapping	43
Configure Identity Mapping	44
Filter Identity Mapping	45
Active Directory Requirements to Support Identity Mapping	46
Configure Active Directory for Identity Mapping	46
Set the Windows Audit Policy	49
Set Permissions When AD User in the Domain Admin Group	49
Required Permissions When AD User Not in Domain Admin Group	50

Permissions to Use DCOM on the Domain Controller	52
Set Permissions for Access to WMI Root/CIMv2 Name Space	54
Grant Access to the Security Event Log on the AD Domain Controller	55
Inline Posture Node	56
Inline Posture Node Installation	57
Cisco ISE Distributed Deployment	57
Cisco ISE Deployment Setup	57
Data Replication from Primary to Secondary ISE Nodes	57
Cisco ISE Node Deregistration	58
Automatic Restart of the Cisco ISE Application Server	58
Guidelines for Setting Up a Distributed Deployment	58
Menu Options Available on Primary and Secondary Nodes	59
Configure a Cisco ISE Node	60
Configure a Primary Administration Node	61
Register a Secondary Cisco ISE Node	61
Register an Inline Posture Node	63
View Nodes in a Deployment	64
Synchronize Primary and Secondary Cisco ISE Nodes	64
Create a Policy Service Node Group	64
Deploy Cisco pxGrid Services	65
Change Node Personas and Services	66
Manually Promote Secondary Administration Node To Primary	66
Configure Primary Administration Node for Automatic Failover	67
Configure Monitoring Nodes for Automatic Failover	68
Remove a Node from Deployment	69
Change the Hostname or IP Address of a Standalone Cisco ISE Node	69
Replace the Cisco ISE Appliance Hardware	70

CHAPTER 4**Set Up Inline Posture 71**

Role of Inline Posture Node in a Cisco ISE Deployment	71
Inline Posture Policy Enforcement	72
Inline Posture Policy Enforcement Flow	72
Trusted and Untrusted Interfaces	74
Dedicated Nodes Required for Inline Posture	74
Standalone Inline Posture Node in a Cisco ISE Deployment	74

Inline Posture High Availability	74
Automatic Failover in Inline Posture Nodes	75
Inline Posture Operating Modes	75
Inline Posture Routed Mode	76
Inline Posture Bridged Mode	76
Inline Posture Maintenance Mode	77
Inline Posture High Availability in Routed and Bridged Modes	77
Best Practices for Inline Posture Deployment	78
Inline Posture Node Guidelines	79
Inline Posture Node Authorization	82
Deploy an Inline Posture Node	84
Configure an Inline Posture Node	84
Create Inline Posture Downloadable Access Control Lists	87
Create Inline Posture Node Profiles	87
Create an Inline Posture Authorization Policy	88
Configure a High-Availability Pair	89
Synchronize an Inline Posture Node	90
Configure Inline Posture Node as RADIUS Client in Administration Node	91
Remove an Inline Posture Node from Deployment	92
Health of an Inline Posture Node	92
Remote Access VPN Use Case	92
Configure an Inline Posture Node with a VPN Device	94
Collection of Inline Posture Node Logs	94
Kclick process in Inline Posture Node	95

PART III
Setup Cisco ISE Management Access 97

CHAPTER 5
Administer Cisco ISE 99

Log in to Cisco ISE	99
Administrator Login Browser Support	100
Administrator Lockout Following Failed Login Attempts	100
Specify Proxy Settings in Cisco ISE	100
Ports Used by the Admin Portal	101
Specify System Time and NTP Server Settings	101
Change the System Time Zone	102

Configure SMTP Server to Support Notifications	103
Install a Software Patch	103
Cisco ISE Software Patches	104
Software Patch Installation Guidelines	104
Roll Back Software Patches	105
Software Patch Rollback Guidelines	105
View Patch Install and Rollback Changes	106
FIPS Mode Support	106
Enable FIPS Mode in Cisco ISE	107
FIPS Mode Operational Parameters	107
Cisco NAC Agent Requirements when FIPS Mode is Enabled	107
Configure Cisco ISE for Administrator CAC Authentication	108
Supported Common Access Card Standards	110
Common Access Card Operation in Cisco ISE	110
Securing SSH Key Exchange Using Diffie-Hellman Algorithm	110
Configure Cisco ISE to Send Secure Syslog	110
Configure Secure Syslog Remote Logging Target	111
Enable Logging Categories to Send Auditable Events to the Secure Syslog Target	112
Disable the TCP Syslog and UDP Syslog Collectors	112

CHAPTER 6

Manage Administrators and Admin Access Policies	113
Role-Based Access Control	113
Cisco ISE Administrators	113
Privileges of a CLI Administrator Versus a Web-Based Administrator	114
Create a New Cisco ISE Administrator	114
Cisco ISE Administrator Groups	114
Create Admin Groups	121
Administrative Access to Cisco ISE	121
Role-Based Access Control in Cisco ISE	122
Role-Based Permissions	122
RBAC Policies	122
Default Menu Access Permissions	122
Configure Menu Access Permissions	124
Default Data Access Permissions	124
Configure Data Access Permissions	125

- Configure Admin Access Policies 125
- Administrator Access Settings 126
 - Configure the Maximum Number of Concurrent Administrative Sessions and Login Banners 126
 - Allow Administrative Access to Cisco ISE from Select IP Addresses 126
 - Configure a Password Policy for Administrator Accounts 127
 - Configure Session Timeout for Administrators 128
 - Terminate an Active Administrative Session 128
 - Change Administrator Name 128
- Administrative Access to Cisco ISE Using an External Identity Store 129
 - External Authentication and Authorization 129
 - External Authentication Process Flow 130
 - Configure a Password-Based Authentication Using an External Identity Store 130
 - Create an External Administrator Group 130
 - Configure Menu Access and Data Access Permissions for the External Administrator Group 131
 - Create an RBAC Policy for External Administrator Authentication 131
 - Configure Admin Access Using an External Identity Store for Authentication with Internal Authorization 132

CHAPTER 7**Cisco ISE Licenses 133**

- Cisco ISE Licenses 133
- License Consumption 135
 - View License Consumption 136
 - Unregistered License Consumption 136
- Manage License Files 137
 - Register Licenses 137
 - Re-Host Licenses 137
 - Renew Licenses 138
 - Migrate and Upgrade Licenses 138
 - Remove Licenses 138

CHAPTER 8**Manage Certificates 141**

- Certificate Management in Cisco ISE 141
 - Certificates Enable Cisco ISE to Provide Secure Access 141

Certificate Usage	142
Certificate Matching in Cisco ISE	142
Validity of X.509 Certificates	143
Enable PKI in Cisco ISE	143
Wildcard Certificates	144
Wildcard Certificate Support in Cisco ISE	145
Wildcard Certificates for HTTPS and EAP Communication	145
Fully Qualified Domain Name in URL Redirection	145
Advantages of Using Wildcard Certificates	146
Disadvantages of Using Wildcard Certificates	146
Wildcard Certificate Compatibility	147
System Certificates	147
View System Certificates	148
Import a System Certificate	149
Generate a Self-Signed Certificate	149
Edit a System Certificate	150
Delete System Certificate	151
Export a System Certificate	151
Trusted Certificates Store	152
Certificates in Trusted Certificates Store	153
Trusted Certificate Naming Constraint	153
View Trusted Store Certificates	154
Change the Status of a Certificate in Trusted Certificates Store	154
Add a Certificate to Trusted Certificates Store	154
Edit a Trusted Certificate	155
Delete Trusted Certificates	155
Export a Certificate from the Trusted Certificates Store	156
Import the Root Certificates to the Trusted Certificate Store	156
Certificate Chain Import	156
Certificate Signing Requests	157
Create a Certificate Signing Request and Submit the CSR to a Certificate Authority	157
Bind the CA-Signed Certificate to the CSR	158
Export a Certificate Signing Request	158
Install Trusted Certificates for Cisco ISE Inter-node Communication	159

Set Up Certificates for Portal Use	160
Reassign Default Portal Certificate Group Tag to CA-Signed Certificate	160
Associate the Portal Certificate Tag Before You Register a Node	161
User and Endpoint Certificate Renewal	162
Dictionary Attributes Used in Policy Conditions for Certificate Renewal	162
Authorization Policy Condition for Certificate Renewal	162
CWA Redirect to Renew Certificates	163
Configure Cisco ISE to Allow Users to Renew Certificates	163
Update the Allowed Protocol Configuration	163
Create an Authorization Policy Profile for CWA Redirection	164
Create an Authorization Policy Rule to Renew Certificates	164
Certificate Renewal Fails for Apple iOS Devices	165
Cisco ISE CA Service	165
Certificates Provisioned on Primary Administration Node and Policy Service Nodes	165
Simple Certificate Enrollment Protocol Profiles	166
Endpoint Certificates	166
Backup and Restore of Cisco ISE CA Certificates and Keys	167
Export Cisco ISE CA Certificates and Keys	167
Import Cisco ISE CA Certificates and Keys	168
Generate Root CA and Subordinate CAs on the PAN and PSN	169
Configure Cisco ISE Root CA as Subordinate CA of an External PKI	169
Configure Cisco ISE to Use Certificates for Authenticating Personal Devices	170
Add Users to the Employee User Group	171
Create a Certificate Authentication Profile for TLS-Based Authentication	171
Create an Identity Source Sequence for TLS-Based Authentication	172
Configure Certificate Authority Settings	172
Create a CA Template	173
Create a Native Supplicant Profile to be Used in Client Provisioning Policy	174
Download Agent Resources from Cisco Site for Windows and MAC OS X Operating Systems	175
Create Client Provisioning Policy Rules for Apple iOS, Android, and MACOSX Devices	175
Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication	176
Create Authorization Profiles for Central Web Authentication and Supplicant Provisioning Flows	176

Create Authorization Policy Rules	177
CA Service Policy Reference	177
Client Provisioning Policy Rules for Certificate Services	177
Authorization Profiles for Certificate Services	179
Authorization Policy Rules for Certificate Services	180
Revoke an Endpoint Certificate	181
OCSP Services	181
Cisco ISE CA Service Online Certificate Status Protocol Responder	181
OCSP Certificate Status Values	182
OCSP High Availability	182
OCSP Failures	182
Add OCSP Client Profiles	183
OCSP Statistics Counters	183

CHAPTER 9**Manage Network Devices 185**

Network Devices Definitions in Cisco ISE	185
Default Network Device Definition in Cisco ISE	186
Create a Network Device Definition in Cisco ISE	187
Import Network Devices into Cisco ISE	187
Export Network Devices from Cisco ISE	188
Network Device Groups	188
Network Device Attributes Used By Cisco ISE in Policy Evaluation	189
Import Network Device Groups in to Cisco ISE	189
Export Network Device Groups from Cisco ISE	190
Import Templates in Cisco ISE	190
Network Devices Import Template Format	191
Network Device Groups Import Template Format	194
Mobile Device Manager Interoperability with Cisco ISE	195
Supported MDM Use Cases	197
Supported MDM Servers	198
Ports Used by the MDM Server	198
MDM Dictionary Attributes	199
MDM Integration Process Flow	199
Set Up MDM Servers With Cisco ISE	201
Import MDM Server Certificate into Cisco ISE	201

Set Permissions When AD User in the Domain Admin Group	201
Required Permissions When AD User Not in Domain Admin Group	202
Permissions to Use DCOM on the Domain Controller	204
Set Permissions for Access to WMI Root/CIMv2 Name Space	206
Open Firewall Ports for WMI Access	207
Configure an Authorization Profile for Redirecting Nonregistered Devices	207
Configure Authorization Policy Rules for the MDM Use Cases	208
Wipe or Lock a Device	209
View Mobile Device Manager Reports	209
View Mobile Device Manager Logs	209

CHAPTER 10
Manage Resources 211

Dictionaries and Dictionary Attributes	211
System Defined Dictionaries and Dictionary Attributes	211
Display System Dictionaries and Dictionary Attributes	212
User-Defined Dictionaries and Dictionary Attributes	212
Create User-Defined Dictionaries	212
Create User-Defined Dictionary Attributes	213
RADIUS-Vendor Dictionaries	213
Create RADIUS-Vendor Dictionaries	214
Create RADIUS-Vendor Dictionary Attributes	214

CHAPTER 11
Logging Mechanism 215

Cisco ISE Logging Mechanism	215
Configure Local Log Purge Settings	216
Cisco ISE System Logs	216
Local Store Syslog Message Format	216
Remote Syslog Message Format	218
Configure Remote Syslog Collection Locations	221
Cisco ISE Message Codes	222
Set Severity Levels for Message Codes	222
Cisco ISE Message Catalogs	222
Debug Logs	222
Configure Debug Log Severity Level	223
Endpoint Debug Log Collector	223

Download Debug Logs for a Specific Endpoint 223

Collection Filters 224

Configure Collection Filters 224

Event Suppression Bypass Filter 224

CHAPTER 12**Backup and Restore Operations 227**

Backup Data Type 227

Backup and Restore Repositories 228

Create Repositories 228

On-Demand and Scheduled Backups 229

Perform an On-Demand Backup 229

Schedule a Backup 231

Backup Using the CLI 233

Backup History 233

Backup Failures 233

Cisco ISE Restore Operation 234

Guidelines for Data Restoration 234

Restoration of Configuration or Monitoring Backup from the CLI 235

Restore Configuration Backups from the GUI 237

Restoration of Monitoring Database 237

Restore a Monitoring Backup in a Standalone Environment 238

Restore a Monitoring Backup with Administration and Monitor Personas 238

Restore a Monitoring Backup with a Monitoring Persona 239

Restore History 239

Export Authentication and Authorization Policy Configuration 240

Synchronize Primary and Secondary Nodes in a Distributed Environment 240

Recovery of Lost Nodes in Standalone and Distributed Deployments 240

Recovery of Lost Nodes Using Existing IP Addresses and Hostnames in a Distributed
Deployment 241

Recovery of Lost Nodes Using New IP Addresses and Hostnames in a Distributed
Deployment 241

Recovery of a Node Using Existing IP Address and Hostname in a Standalone
Deployment 242

Recovery of a Node Using New IP Address and Hostname in a Standalone
Deployment 242

- Configuration Rollback 243
- Recovery of Primary Node in Case of Failure in a Distributed Deployment 243
- Recovery of Secondary Node in Case of Failure in a Distributed Deployment 243

CHAPTER 13
Setup Endpoint Protection ServiceAdaptive Network Control 245

- Enable Endpoint Protection Service Adaptive Network Control in Cisco ISE 245
- Configure Network Access Settings 245
 - Quarantined Endpoints Do Not Renew Authentication Following Policy Change 246
- Endpoint Protection ServiceAdaptive Network Control 247
 - Create Authorization Profiles for Network Access through EPSANC 248
 - Create Exception Policies for Network Access through EPSANC 248
 - EPSANC Operations Fail when IP Address or MAC Address is not Found 248
 - Externally Authenticated Administrators Cannot Perform EPSANC Operations 249
- EPSANC Quarantine and Unquarantine Flow 249
- EPSANC NAS Port Shutdown Flow 250
- Endpoints Purge Settings 250

PART IV
Manage Users and End-User Portals 253

CHAPTER 14
Manage Users and External Identity Sources 255

- Cisco ISE Users 255
 - User Identity 255
 - User Groups 256
 - User Identity Groups 256
 - User Role 256
 - User Account Custom Attributes and Password Policies 256
- Add Users 258
- Export Cisco ISE User Data 258
- Import Cisco ISE User Data 259
- Create a User Identity Group 259
- Export User Identity Groups 259
- Import User Identity Groups 260
- Internal and External Identity Sources 260
 - Create an External Identity Source 261
- Certificate Authentication Profiles 262

Add a Certificate Authentication Profile	262
Active Directory as an External Identity Source	263
Active Directory Supported Authentication Protocols and Features	263
Active Directory Attribute and Group Retrieval for Use in Authorization Policies	264
Active Directory Certificate Retrieval for Certificate-Based Authentication	264
Active Directory User Authentication Process Flow	265
Support for Active Directory Multidomain Forests	265
Prerequisites for Integrating Active Directory and Cisco ISE	265
Active Directory Account Permissions Required for Performing Various Operations	266
Network Ports That Must Be Open for Communication	267
DNS Server	267
Configure Active Directory as an External Identity Source	267
Add an Active Directory Join Point and Join Cisco ISE Node to the Join Point	268
Leave the Active Directory Domain	269
Configure Authentication Domains	270
Configure Active Directory User Groups	271
Configure Active Directory User and Machine Attributes	272
Modify Password Changes, Machine Authentications, and Machine Access Restriction Settings	272
Support for Active Directory Multi-Join Configuration	272
Create a New Scope to Add Active Directory Join Points	273
Identity Rewrite	273
Enable Identity Rewrite	275
Identity Resolution Settings	275
Avoid Identity Resolution Issues	275
Configure Identity Resolution Settings	276
Test Users for Active Directory Authentication	277
Delete Active Directory Configurations	277
View Active Directory Joins for a Node	278
Diagnose Active Directory Problems	278
Enable Active Directory Debug Logs	279
Obtain the Active Directory Log File for Troubleshooting	279
Active Directory Alarms and Reports	279
Active Directory Advanced Tuning	280

Supplemental Information for Setting Up Cisco ISE with Active Directory	280
Configure Group Policies in Active Directory	280
Configure Odyssey 5.X Supplciant for EAP-TLS Machine Authentications Against Active Directory	281
AnyConnect Agent for Machine Authentication	282
ISE pxGrid Identity Mapping	282
Configure Identity Mapping	283
Filter Identity Mapping	284
Active Directory Requirements to Support Identity Mapping	284
Configure Active Directory for Identity Mapping	284
Set the Windows Audit Policy	288
Set Permissions When AD User in the Domain Admin Group	288
Required Permissions When AD User Not in Domain Admin Group	289
Permissions to Use DCOM on the Domain Controller	291
Set Permissions for Access to WMI Root/CIMv2 Name Space	293
Grant Access to the Security Event Log on the AD Domain Controller	294
LDAP	295
LDAP Directory Service	295
Multiple LDAP Instances	296
LDAP Failover	296
LDAP Connection Management	296
LDAP User Authentication	297
LDAP Group and Attribute Retrieval for Use in Authorization Policies	297
LDAP Group Membership Information Retrieval	297
LDAP Attributes Retrieval	298
LDAP Certificate Retrieval	298
Errors Returned by the LDAP Server	298
LDAP User Lookup	299
LDAP MAC Address Lookup	299
Add LDAP Identity Sources	300
Configure Primary and Secondary LDAP Servers	300
Enable Cisco ISE to Obtain Attributes from the LDAP Server	300
Retrieve Group Membership Details from the LDAP Server	301
Retrieve User Attributes From the LDAP Server	302
Enable Secure Authentication with LDAP Identity Source	302

RADIUS Token Identity Sources	303
RADIUS Token Server Supported Authentication Protocols	303
Ports Used By the RADIUS Token Servers for Communication	303
RADIUS Shared Secret	303
Failover in RADIUS Token Servers	304
Configurable Password Prompt in RADIUS Token Servers	304
RADIUS Token Server User Authentication	304
User Attribute Cache in RADIUS Token Servers	304
RADIUS Identity Source in Identity Sequence	304
RADIUS Server Returns the Same Message for All Errors	304
Safeword Server Supports Special Username Format	305
Authentication Request and Response in RADIUS Token Servers	305
Add a RADIUS Token Server	306
Delete a RADIUS Token Server	307
RSA Identity Sources	307
Cisco ISE and RSA SecurID Server Integration	308
RSA Configuration in Cisco ISE	308
RSA Agent Authentication Against the RSA SecurID Server	308
RSA Identity Sources in a Distributed Cisco ISE Environment	308
RSA Server Updates in a Cisco ISE Deployment	308
Override Automatic RSA Routing	308
RSA Node Secret Reset	309
RSA Automatic Availability Reset	309
Add RSA Identity Sources	309
Import the RSA Configuration File	309
Configure the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files	310
Configure Authentication Control Options for RSA Identity Source	311
Configure RSA Prompts	311
Configure RSA Messages	311
SAMLv2 Identity Provider as an External Identity Source	312
Add a SAML Identity Provider	313
Delete an Identity Provider	315
Authentication Failure Log	316
Identity Source Sequences	316

Create Identity Source Sequences	316
Delete Identity Source Sequences	317
Identity Source Details in Reports	317
Authentications Dashlet	318
Identity Source Reports	318

CHAPTER 15
Configure Guest Access 319

Cisco ISE Guest Services	319
End-User Guest and Sponsor Portals in Distributed Environment	319
Guest and Sponsor Accounts	320
Guest Accounts	320
Manage Guest Accounts on the Sponsor Portal	321
Guest Types and User Identity Groups	321
Create or Edit Guest Types	322
Disable Guest Types	325
Changing Guest Account Attributes	326
Configure Maximum Simultaneous Logins for Endpoint Users	326
Schedule When to Purge Expired Guest Accounts	327
Add Custom Fields for Guest Account Creation	328
Specify Email Addresses and SMTP Servers for Email Notifications	329
Assign Guest Locations and SSIDs	329
Rules for Guest Password Policies	330
Set the Guest Password Policy and Expiration	331
Rules for Guest Username Policies	332
Set the Guest Username Policy	332
SMS Providers and Services	333
Configure SMS Gateways to Send SMS Notifications to Guests	333
Managing Sponsor Accounts	334
Sponsor Groups	335
Create Sponsor Accounts and Assign to Sponsor Groups	335
Configure Sponsor Groups	336
Guest Portals	338
Credentials for Guest Portals	338
Guest Access with Hotspot Guest Portals	339
Guest Access with Credentialed Guest Portals	340

Employee Access with Credentialed Guest Portals	340
Configure Periodic AUP Acceptance	340
Guest Device Compliance	341
Guest Portals Configuration Tasks	341
Enable Policy Services	342
Add Certificates for Guest Portals	342
Create External Identity Sources	343
Create Identity Source Sequences	343
Create Endpoint Identity Groups	344
Create a Hotspot Guest Portal	344
Create a Sponsored-Guest Portal	345
Create a Self-Registered Guest Portal	347
Authorize Portals	349
Create Authorization Profiles	349
Create Authorization Policy Rules for Hotspot and MDM Portals	349
Customize Guest Portals	350
Sponsor Portals	350
Configure a Sponsor Portal	350
Enable Policy Services	351
Add Certificates for Guest Services	351
Create External Identity Sources	352
Create Identity Source Sequences	352
Create a Sponsor Portal	353
Customize Sponsor Portals	354
Sponsors Cannot Log In to the Sponsor Portal	354
Monitor Guest and Sponsor Activity	354
Metrics Dashboard	355
AUP Acceptance Status Report	355
Guest Accounting Report	355
Master Guest Report	355
Sponsor Login and Audit Report	356
Audit Logging for Guest and Sponsor Portals	356
Guest Access Deployment Scenarios	356
NAD with Central WebAuth Process	356
Wireless LAN Controller with Local WebAuth Process	358

Wired NAD with Local WebAuth Process	359
IP Address and Port Values Required for the Login.html Page	360
HTTPS Server Enabled on the NAD	360
Support for Customized Authentication Proxy Web Pages on the NAD	360
Configure Web Authentication on the NAD	360
Device Registration WebAuth Process	361

CHAPTER 16**Support Device Access 365**

Personal Devices on a Corporate Network	365
End-User Device Portals in a Distributed Environment	365
Limit the Number of Personal Devices Registered by Employees	366
Employee Accounts	366
Personal Device Portals	366
Access Device Portals	367
Blacklist Portal	367
Bring Your Own Device Portal	367
Client Provisioning Portal	368
Mobile Device Management Portal	368
My Devices Portal	368
Support Device Registration Using Native Supplicants	369
BYOD Deployment Scenarios for Personal Devices Using Native Supplicants	369
Operating Systems Supported by Native Supplicants	370
Allow Employees to Register Personal Devices Using Credentialed Guest Portals	371
Provide a URL to Reconnect with BYOD Registration	371
Device Portals Configuration Tasks	371
Enable Policy Services	373
Add Certificates	373
Create External Identity Sources	374
Create Identity Source Sequences	374
Create Endpoint Identity Groups	375
Edit the Blacklist Portal	375
Create a BYOD Portal	376
Create a Client Provisioning Portal	378
Create an MDM Portal	379
Create a My Devices Portal	380

Authorize Portals	381
Create Authorization Profiles	381
Create Authorization Policy Rules	382
Customize Device Portals	382
Manage Personal Devices Added by Employees	382
Display Devices Added by an Employee	383
Errors When Adding Devices to My Devices Portal	383
Devices Deleted from My Devices Portal Remain in Endpoints Database	383
Monitor My Devices Portals and Endpoints Activity	383
My Devices Login and Audit Report	384
Registered Endpoints Report	384

CHAPTER 17
Customize End-User Web Portals 385

End-User Portals	385
Customization of End-User Web Portals	385
Portal Themes, Images, and Banners	388
Portal Page Titles, Content, and Labels	389
Basic Customization of Portals	389
Modify the Portal Theme Colors	389
Change the Portal Display Language	390
Change the Portal Icons, Images, and Logos	391
Update the Portal Banner and Footer Elements	391
Change the Titles, Instructions, Buttons, and Label Text	392
Format and Style Text Box Content	392
View Your Customization	393
Custom File Upload	393
Advanced Customization of Portals	394
Configure Portal Customization	394
Portal Theme and Structure CSS Files	394
About Changing Theme Colors with jQuery Mobile	395
Change Theme Colors with jQuery Mobile	397
Location Based Customization	398
User Device Type Based Customization	399
Export a Portal's Default Theme CSS File	399
Create a Custom Portal Theme CSS File	400

Embed Links in Portal Content	400
Insert Variables for Dynamic Text Updates	401
Use Source Code to Format Text and Include Links	402
Add an Image as an Advertisement	403
Set Up Carousel Advertising	404
Customize Greetings Based on Guest Location	406
Customize Greetings Based on User Device Type	407
Modify the Portal Page Layout	408
Import the Custom Portal Theme CSS File	411
Delete a Custom Portal Theme	411
View Your Customization	412
Customization of a Portal Language File	412
Export the Language File	413
Add or Delete Languages from the Language File	413
Import the Updated Language File	414
Customization of Guest Notifications, Approvals, and Error Messages	414
Customize Email Notifications	415
Customize SMS Text Message Notifications	415
Customize Print Notifications	416
Customize Approval Request Email Notifications	417
Edit Error Messages	417

PART V**Enable and Configure Cisco ISE Services 419**

CHAPTER 18**Set Up Policy Conditions 421**

Policy Conditions	421
Simple and Compound Conditions	421
Policy Evaluation	422
Create Simple Conditions	422
Create Compound Conditions	423
Profiler Conditions	424
Create a Profiler Condition	424
Posture Conditions	425
Simple Posture Conditions	425
Create Simple Posture Conditions	425

Compound Posture Conditions	426
Cisco-Predefined Condition for Enabling Automatic Updates in Windows Clients	426
Cisco-Preconfigured Antivirus and Antispyware Conditions	426
Antivirus and Antispyware Support Chart	426
Create Compound Posture Conditions	427
Create Patch Management Conditions	427
Create Time and Date Conditions	428

CHAPTER 19

Manage Authentication Policies	429
Cisco ISE Authentication Policies	429
Policy Condition Evaluation	430
Supported Authentication Protocols	430
Supported Authentication Types and Database	430
Types of Authentication Failures	431
Authentication Policy Terminology	431
Simple Authentication Policies	432
Simple Authentication Policy Flow	433
Guidelines for Configuring Simple Authentication Policies	434
Rule-Based Authentication Policies	434
Rule-Based Authentication Policy Flow	434
Supported Dictionaries for Rule-Based Authentication Policies	435
Attributes Supported by Dictionaries	436
Protocol Settings for Authentication	439
Guidelines for Using EAP-FAST as Authentication Protocol	439
Configure EAP-FAST Settings	440
Generate the PAC for EAP-FAST	440
Configure EAP-TLS Settings	440
Configure PEAP Settings	441
Configure RADIUS Settings	441
Network Access Service	441
Define Allowed Protocols for Network Access	441
Enable MAB from Non-Cisco Devices	443
Enable MAB from Cisco Devices	443
Cisco ISE Acting as a RADIUS Proxy Server	444

Configure External RADIUS Servers	445
Define RADIUS Server Sequences	445
Policy Modes	446
Change Policy Modes	446
Configure a Simple Authentication Policy	447
Configure a Rule-Based Authentication Policy	447
Default Authentication Policy	449
Policy Sets	449
Policy Set Evaluation Flow	450
Guidelines for Creating Policy Sets	450
Global Authorization Exception Policy	451
Configure Policy Sets	451
Authentication Policy Built-In Configurations	451
View Authentication Results	453
Authentication Dashlet	454
Authentication Reports and Troubleshooting Tools	454

CHAPTER 20

Manage Authorization Policies and Profiles	455
Cisco ISE Authorization Policies	455
Cisco ISE Authorization Profiles	455
Authorization Policy Terminology	456
Network Authorization	456
Policy Elements	456
Authorization Profile	456
Authorization Policy	457
Access Control Lists	457
Authorization Policies and Supported Dictionaries	458
Guidelines for Configuring Authorization Policies and Profiles	458
Default Authorization Policy, Rule, and Profile Configuration	459
Configure Authorization Policies	462
Authorization Policy Attributes and Conditions	463
Time and Date Conditions	464
Permissions for Authorization Profiles	464
Configure Permissions for New Standard Authorization Profiles	465
Downloadable ACLs	465

Configure Permissions for Downloadable ACLs	465
Supported Downloadable ACL Format for Inline Posture Node	465
Machine Access Restriction for Active Directory User Authorization	467

CHAPTER 21

Cisco ISE Endpoint Profiling Policies	469
Cisco ISE Profiling Service	469
Endpoint Inventory Using Profiling Service	470
Cisco ISE Profiler Queue Limit Configuration	470
Configure Profiling Service in Cisco ISE Nodes	471
Network Probes Used by Profiling Service	471
IP Address and MAC Address Binding	472
NetFlow Probe	472
DHCP Probe	473
Wireless LAN Controller Configuration in DHCP Bridging Mode	473
DHCP SPAN Probe	473
HTTP Probe	474
HTTP SPAN Probe	474
Unable to Collect HTTP Attributes in Cisco ISE Running on VMware	474
RADIUS Probe	474
Network Scan (NMAP) Probe	475
SNMP Read Only Community Strings for NMAP Manual Subnet Scan	475
Latest Network Scan Results	476
DNS Probe	476
DNS FQDN Lookup	476
DNS Lookup with an Inline Posture Node Deployment in Bridged Mode	477
Configure Call Station ID Type in the WLC Web Interface	477
SNMP Query Probe	477
Cisco Discovery Protocol Support with SNMP Query	478
Link Layer Discovery Protocol Support with SNMP Query	478
CDP and LLDP Capability Codes Displayed in a Single Character	478
SNMP Trap Probe	479
Configure Probes per Cisco ISE Node	479
Setup CoA, SNMP RO Community, and Endpoint Attribute Filter	480
Global Configuration of Change of Authorization for Authenticated Endpoints	481
Use Cases for Issuing Change of Authorization	481

Exemptions for Issuing a Change of Authorization	482
Change of Authorization Issued for Each Type of CoA Configuration	483
Attribute Filters for ISE Database Persistence and Performance	483
Global Setting to Filter Endpoint Attributes with Whitelist	484
Attributes Collection from IOS Sensor Embedded Switches	486
IOS Sensor Embedded Network Access Devices	486
Configuration Checklist for IOS Sensor-Enabled Network Access Devices	486
Endpoint Profiling Policy Rules	487
Create Endpoint Profiling Policies	488
Change of Authorization Configuration per Endpoint Profiling Policy	489
Import Endpoint Profiling Policies	490
Export Endpoint Profiling Policies	490
Predefined Endpoint Profiling Policies	491
Predefined Endpoint Profiling Policies Overwritten During Upgrade	492
Unable to Delete Endpoint Profiling Policies	492
Predefined Profiling Policies for Draeger Medical Devices	492
Endpoint Profiling Policy for Unknown Endpoints	493
Endpoint Profiling Policy for Statically Added Endpoints	493
Endpoint Profiling Policy for Static IP Devices	493
Endpoint Profiling Policy Matching	493
Endpoint Profiling Policies Used for Authorization	494
Endpoint Profiling Policies Grouped into Logical Profiles	494
Create Logical Profiles	494
Profiling Exception Actions	495
Create Exception Actions	495
Profiling Network Scan Actions	495
Create a New Network Scan Action	496
NMAP Operating System Scan	496
Operating System Ports	497
NMAP SNMP Port Scan	501
NMAP Common Ports Scan	502
Common Ports	502
Cisco ISE Integration with Cisco NAC Appliance	503
Cisco Clean Access Manager Configuration in Administration Nodes	503
Cisco ISE Profiler and Cisco Clean Access Manager Communication	503

Add Cisco Clean Access Managers	504
Create Endpoints with Static Assignments of Policies and Identity Groups	504
Import Endpoints from CSV Files	505
Default Import Template Available for Endpoints	506
Unknown Endpoints Reprofiled During Import	506
Static Assignments of Policies and Identity Groups for Endpoints Retained During Import	507
Endpoints with Invalid Attributes Not Imported	507
Import Endpoints from LDAP Server	508
Export Endpoints with Comma-Separated Values File	508
Identified Endpoints	509
Identified Endpoints Locally Stored in Policy Service Nodes Database	509
Policy Service Nodes in Cluster	510
Create Endpoint Identity Groups	511
Identified Endpoints Grouped in Endpoint Identity Groups	511
Default Endpoint Identity Groups Created for Endpoints	511
Endpoint Identity Groups Created for Matched Endpoint Profiling Policies	512
Add Static Endpoints in Endpoint Identity Groups	512
Dynamic Endpoints Reprofiled After Adding or Removing in Identity Groups	513
Endpoint Identity Groups Used in Authorization Rules	513
Profiler Feed Service	513
OUI Feed Service	514
Configure Profiler Feed Service	514
Remove Updates to Endpoint Profiling Policies	515
Profiler Reports	516

CHAPTER 22

Configure Client Provisioning	517
Enable Client Provisioning in Cisco ISE	518
Client Provisioning Resources	518
Add Client Provisioning Resources from Cisco	519
Download Client Provisioning Resources Automatically	519
Add Cisco Provided Client Provisioning Resources from a Local Machine	520
Add Customer Created Resources for AnyConnect from a Local Machine	521
Configure Personal Device Registration Behavior	522
Create Native Supplicant Profiles	522

Native Supplicant Profile Settings	523
AMP Enabler Profile Settings	524
Create an AMP Enabler Profile Using the Embedded Profile Editor	525
Create an AMP Enabler Profile Using the Standalone Editor	525
Troubleshoot Common AMP Enabler Installation Errors	527
Create AnyConnect Configuration	527
Create AnyConnect and Cisco NAC Agent Profiles	528
Agent Profile Configuration Guidelines	529
Agent Behavior Configuration	529
Supported Languages	534
Client IP Address Refresh Configuration	535
Posture Protocol Settings	540
Client Login Session Criteria	543
Agent Download Issues on Client Machine	543
Provision Client Machines with the Cisco NAC Agent MSI Installer	544
Cisco ISE Posture Agents	545
Posture Agent Discovery Request and Cisco ISE Response	545
Web Agent Posture Discovery Request and Cisco ISE Response	545
Agent Displays “Temporary Access”	546
Agent Fails to Initiate Posture Assessment	546
AnyConnect	546
Cisco NAC Agent XML File Installation Directories	547
Cisco NAC Agent for Windows Clients	547
Uninstall the Cisco NAC Agent from Windows 7 and Earlier Clients	547
Uninstall the Cisco NAC Agent in a Windows 8 Client	548
Windows 8 Metro and Metro App Support —Toast Notifications	548
Cisco NAC Agent for Macintosh Clients	549
Uninstall the Cisco NAC Agent from Macintosh Clients	549
Cisco Web Agent	549
Cisco NAC Agent Logs	550
Create an Agent Customization File for the Cisco NAC Agent	550
Custom nac_login.xml File Template	550
Custom nacStrings_xx.xml File Template	551
Sample Extended nacStrings_xx.xml File	559
UpdateFeed.xml Descriptor File Template	560

- Example XML File Generated Using the Create Profile Function 561
- Configure Client Provisioning Resource Policies 561
 - Configure Cisco ISE Posture Agent in the Client Provisioning Policy 563
 - Configure Native Supplicants for Personal Devices 563
- Client Provisioning Reports 564
- Client Provisioning Event Logs 564

CHAPTER 23

- Configure Client Posture Policies 565**
 - Posture Service 565
 - Components of Posture Services 566
 - Posture and Client-Provisioning Policies Workflow 567
 - Posture Service Licenses 567
 - Posture Service Deployment 567
 - Enable Posture Session Service in Cisco ISE 568
 - Run the Posture Assessment Report 568
 - Posture Administration Settings 568
 - Timer Settings for Clients 569
 - Set Remediation Timer for Clients to Remediate within Specified Time 569
 - Set Network Transition Delay Timer for Clients to Transition 569
 - Set Login Success Screen to Close Automatically 570
 - Set Posture Status for Non-Agent Devices 570
 - Posture Lease 570
 - Periodic Reassessments 571
 - Configure Periodic Reassessments 571
 - Download Posture Updates to Cisco ISE 572
 - Download Posture Updates Automatically 572
 - Configure Acceptable Use Policies for Posture Assessment 573
 - Configure Posture Policies 573
 - Posture Assessment Options 574
 - Posture Remediation Options 575
 - Custom Conditions for Posture 576
 - Custom Posture Remediation Actions 576
 - Add a File Remediation 577
 - Add a Link Remediation 577
 - Add a Patch Management Remediation 577

Add an Antivirus Remediation	578
Add an Antispyware Remediation	578
Add a Launch Program Remediation	579
Troubleshoot Launch Program Remediation	579
Windows Update Remediation	580
Add a Windows Update Remediation	580
Add a Windows Server Update Services Remediation	581
Posture Assessment Requirements	581
Client System Stuck in Noncompliant State	583
Create Client Posture Requirements	583
Custom Permissions for Posture	584
Configure Standard Authorization Policies	584

CHAPTER 24

Cisco TrustSec Policies Configuration	587
TrustSec Architecture	587
TrustSec Components	588
TrustSec Terminology	589
Supported Switches and Required Components for TrustSec	590
Configure TrustSec Global Settings	590
Configure TrustSec Devices	591
OOB TrustSec PAC	591
Generate a TrustSec PAC from the Settings Screen	592
Generate a TrustSec PAC from the Network Devices Screen	592
Generate a TrustSec PAC from the Network Devices List Screen	593
Push Button	593
Configure TrustSec AAA Servers	593
Security Groups Configuration	594
Add Security Groups	594
Import Security Groups into Cisco ISE	595
Export Security Groups from Cisco ISE	596
Add Security Group Access Control Lists	596
Egress Policy	597
Source Tree View	597
Destination Tree View	597
Matrix View	597

Matrix Dimensions	598
Condensed View	598
Import/Export Matrix	598
Matrix Operations	598
Configure SGACL from Egress Policy	599
Egress Policy Table Cells Configuration	599
Add the Mapping of Egress Policy Cells	599
Export Egress Policy	600
Import Egress Policy	600
Configure SGT from Egress Policy	601
Monitor Mode	601
Features of Monitor Mode	601
The Unknown Security Group	601
Default Policy	602
Push Button	602
SGT Assignment	602
NDAC Authorization	602
Configure NDAC Authorization	603
Configure End User Authorization	603
Add Single IP-to-SGT Mappings	604
Add Group IP-to-SGT Mappings	604
Import Security Group Mappings Hosts	605
Export Security Group Mappings Hosts	605
Deploy IP-to-SGT Mappings	605
TrustSec Configuration and Policy Push	606
CoA Supported Network Devices	606
Push Configuration Changes to Non-CoA Supporting Devices	607
SSH Key Validation	607
Environment CoA Notification Flow	609
Environment CoA Triggers	609
Trigger Environment CoA for Network Devices	610
Trigger Environment CoA for Security Groups	610
Trigger Environment CoA for TrustSec AAA Servers	610
Trigger Environment CoA for NDAC Policy	611
Update SGACL Content Flow	611

Initiate an Update SGACL Named List CoA	612
Policies Update CoA Notification Flow	612
Update SGT Matrix CoA Flow	613
Initiate Update SGT Matrix CoA from Egress Policy	613
TrustSec CoA Summary	614
Run Top N RBACL Drops by User Report	615

PART VI
Monitoring and Troubleshooting Cisco ISE 617

CHAPTER 25
Monitoring and Troubleshooting 619

Monitoring and Troubleshooting Service in Cisco ISE	619
Cisco ISE Dashboard	620
Network Privilege Framework	620
NPF Event Flow Process	620
User Roles and Permissions for Monitoring and Troubleshooting Capabilities	621
Data Stored in Monitoring Database	621
Device Configuration for Monitoring	621
Network Process Status	621
Monitor Network Process Status	622
Network Authentications	622
Monitor Network Authentications	622
Profiler Activity and Profiled Endpoints	622
Determine Profiler Activity and Profiled Endpoints	623
Troubleshooting the Profiler Feed	623
Posture Compliance	623
Check Posture Compliance	624
Cisco ISE Alarms	624
Add Custom Alarms	634
Cisco ISE Alarm Notifications and Thresholds	634
Enable and Configure Alarms	635
Cisco ISE Alarms for Monitoring	635
View Monitoring Alarms	635
Log Collection	635
Alarm Syslog Collection Location	636
Live Authentications	636

Monitor Live Authentications	637
Filter Data in Live Authentications Page	637
Global Search for Endpoints	638
Session Trace for an Endpoint	639
Session Removal from the Directory	641
Authentication Summary Report	641
Troubleshoot Network Access Issues	642
Diagnostic Troubleshooting Tools	642
RADIUS Authentication Troubleshooting Tool	642
Troubleshoot Unexpected RADIUS Authentication Results	643
Execute Network Device Tool	643
Execute IOS Show Commands to Check Configuration	643
Evaluate Configuration Validator Tool	643
Troubleshoot Network Device Configuration Issues	644
Posture Troubleshooting Tool	644
Troubleshoot Endpoint Posture Failure	644
TCP Dump Utility to Validate the Incoming Traffic	644
Use TCP Dump to Monitor Network Traffic	645
Save a TCP Dump File	645
Compare Unexpected SGACL for an Endpoint or User	646
Egress Policy Diagnostic Flow	646
Troubleshoot Connectivity Issues in a Trustsec-Enabled Network with SXP-IP Mappings	647
Troubleshoot Connectivity Issues in a Trustsec-Enabled Network with IP-SGT Mappings	647
Device SGT Tool	647
Troubleshoot Connectivity Issues in a Trustsec-Enabled Network by Comparing Device SGT Mappings	648
Download Endpoint Statistical Data From Monitoring Nodes	648
Obtaining Additional Troubleshooting Information	648
Cisco ISE Support Bundle	649
Support Bundle	650
Download Cisco ISE Log Files	650
Cisco ISE Debug Logs	650
Obtain Debug Logs	651

Cisco ISE Components and the Corresponding Debug Logs 651

Download Debug Logs 653

Monitoring Database 653

Back Up and Restore of the Monitoring Database 653

Monitoring Database Purge 654

Guidelines for Purging the Monitoring Database 654

Purge Older Monitoring Data 654

CHAPTER 26**Reports 657**

Cisco ISE Reports 657

Run and View Reports 658

Reports Navigation 658

Export Reports 658

Schedule and Save Cisco ISE Reports 659

Add Favorite Reports 660

Cisco ISE Active RADIUS Sessions 660

Change Authorization for RADIUS Sessions 661

Available Reports 662

PART VII**Reference 675**

CHAPTER 27**Administration User Interface Reference 677**

System Administration 677

Deployment Settings 677

Deployment Nodes List Page 677

General Node Settings 678

Profiling Node Settings 680

Inline Posture Node Settings 682

Certificate Store Settings 686

Endpoint Certificate Overview Page 686

Self-Signed Certificate Settings 687

Certificate Signing Request Settings 688

System Certificate Import Settings 692

Trusted Certificate Store Page 693

Trusted Certificate Edit Settings 694

Trusted Certificate Import Settings	695
OCSP Client Profile Settings	696
Internal CA Settings	698
Certificate Template Settings	699
Logging Settings	700
Remote Logging Target Settings	700
Logging Category Settings	701
Maintenance Settings	701
Repository Settings	702
On-Demand Backup Settings	702
Scheduled Backup Settings	703
Admin Access Settings	703
Administrator Password Policy Settings	703
Session Timeout and Session Info Settings	705
Settings	705
Posture General Settings	705
Posture Reassessment Configuration Settings	706
Posture Acceptable Use Policy Configuration Settings	708
EAP-FAST Settings	709
Generate PAC for EAP-FAST Settings	710
EAP-TLS Settings	711
PEAP Settings	711
RADIUS Settings	711
TrustSec Settings	713
SMS Gateway Settings	713
Identity Management	715
Endpoints	715
Endpoint Settings	715
Endpoint Import from LDAP Settings	717
Groups	718
Endpoint Identity Group Settings	718
External Identity Sources	719
LDAP Identity Source Settings	719
RADIUS Token Identity Sources Settings	725
RSA SecurID Identity Source Settings	726

Identity Management Settings	727
User Password Policy Settings	727
Network Resources	729
Network Devices	729
Network Device Definition Settings	729
Default Network Device Definition Settings	735
Network Device Import Settings	736
Network Device Groups	737
Network Device Group Settings	737
Network Device Group Import Settings	737
External RADIUS Server Settings	738
RADIUS Server Sequences	739
NAC Manager Settings	741
Device Portal Management	741
Configure Device Portal Settings	741
Global Settings for Device Portals	741
Portal Identification Settings for Device Portals	742
Portal Settings for the Blacklist Portal	743
Portal Settings for BYOD Device Registration and MDM Portals	744
BYOD Settings for BYOD Portals	745
Portal Settings for Client Provisioning Portals	746
Employee Mobile Device Management Settings for MDM Portals	747
Portal Settings for My Devices Portals	747
Login Page Settings for My Devices Portals	748
Acceptable Use Policy (AUP) Page Settings for My Devices Portals	749
Post-Login Banner Page Settings for My Devices Portals	750
Employee Change Password Settings for My Devices Portals	750
Manage Device Settings for My Devices Portal	750
Add, Edit, and Locate Device Customization for My Devices Portals	752
Support Information Page Settings for Device Portals	752
CHAPTER 28	Guest Access User Interface Reference 755
Guest Portal Settings	755
Portal Identification Settings	755
Portal Settings for Hotspot Guest Portals	756

Acceptable Use Policy (AUP) Page Settings for Hotspot Guest Portals	758
Post-Access Banner Page Settings for Hotspot Portals	758
Portal Settings for Credentialed Guest Portals	758
Login Page Settings for Credentialed Guest Portals	760
Self-Registration Page Settings for Credentialed Guest Portals	761
Self Registration Success Page Settings for Credentialed Guest Portals	766
Acceptable Use Policy (AUP) Page Settings for Credentialed Guest Portals	767
Guest Change Password Settings for Credentialed Guest Portals	768
Guest Device Registration Settings for Credentialed Guest Portals	769
BYOD Settings for Credentialed Guest Portals	769
Post-Login Banner Page Settings for Credentialed Guest Portals	771
Guest Device Compliance Settings for Credentialed Guest Portals	771
VLAN DHCP Release Page Settings for Guest Portals	772
Authentication Success Settings for Guest Portals	773
Support Information Page Settings for Guest Portals	774
Sponsor Portal Application Settings	775
Portal Identification Settings	775
Portal Settings for Sponsor Portals	776
Login Settings for Sponsor Portals	777
Acceptable Use Policy (AUP) Settings for Sponsor Portals	778
Sponsor Change Password Settings for Sponsor Portals	779
Post-Login Banner Settings for Sponsor Portals	779
Support Information Page Settings for Sponsor Portals	779
Notify Guests Customization for Sponsor Portals	780
Manage and Approve Customization for Sponsor Portals	781
Global Settings	781
Global Settings for Guest and Sponsor Portals	781
Guest Type Settings	782
Sponsor Group Settings	785

CHAPTER 29
Web Portals Customization Reference 789

Portal Pages Titles, Content and Labels Character Limits	789
Character Limits for Portal Pages Titles, Content and Labels	789
Portal Customization	791
CSS Classes and Descriptions for End-User Portals Page Layout	791

HTML Support for a Portal Language File	792
HTML Support for the Blacklist Portal Language File	793
HTML Support for Bring Your Own Device Portals Language Files	793
HTML Support for Client Provisioning Portals Language Files	794
HTML Support for Credential Guest Portals Language Files	795
HTML Support for Hotspot Guest Portals Language Files	798
HTML Support for Mobile Device Management Portals Language Files	798
HTML Support for My Devices Portals Language Files	799
HTML Support for Sponsor Portals Language Files	800
Custom Guest Notifications	801
List of Variables for Portal Pages Customization	802

CHAPTER 30
Policy User Interface Reference 807

Authentication	807
Simple Authentication Policy Configuration Settings	807
Rule-Based Authentication Policy Configuration Settings	808
Authorization Policy Settings	810
Endpoint Profiling Policies Settings	811
Dictionaries	814
Conditions	816
Profiler Condition Settings	816
Posture Conditions Settings	816
File Condition Settings	816
Registry Condition Settings	820
Application Condition Settings	821
Service Conditions Settings	822
Posture Compound Condition Settings	822
Antivirus Compound Condition Settings	823
Antispyware Compound Condition Settings	825
Dictionary Simple Conditions Settings	826
Dictionary Compound Condition Settings	827
Patch Management Condition Settings	828
Time and Date Condition Settings	829
Results	829
Allowed Protocols	830

PAC Options	834
Authorization Profile Settings	837
Profiling Exception Action Settings	840
File Remediation	840
Link Remediation	841
Antivirus Remediation	841
Antispyware Remediation	842
Launch Program Remediation	843
Windows Update Remediation	844
Windows Server Update Services Remediation	845
Patch Management Remediation	847
Client Posture Requirements	848

CHAPTER 31**Operations User Interface Reference 851**

Recent RADIUS Authentications	851
Show Live Sessions	852
Diagnostic Tools	854
RADIUS Authentication Troubleshooting Settings	854
Execute Network Device Command Settings	855
Evaluate Configuration Validator Settings	855
Posture Troubleshooting Settings	856
TCP Dump Settings	857
SXP-IP Mappings	858
IP User SGT	859
Device SGT Settings	860
Progress Details Settings	861
Results Summary	862

CHAPTER 32**Network Access Flows 863**

Password-Based Authentication	863
Secure Authentication Using Encrypted Passwords and Cryptographic Techniques	863
Authentication Methods and Authorization Privileges	864
RADIUS Protocol Support in Cisco ISE	864
Network Access for Users	864
RADIUS-Based Protocols Without EAP	864

RADIUS-Based Non-EAP Authentication Flow	865
Password Authentication Protocol	865
RADIUS-Based PAP Authentication in Cisco ISE	865
Challenge Handshake Authentication Protocol	866
Microsoft Challenge Handshake Authentication Protocol Version 1	866
Microsoft Challenge Handshake Authentication Protocol Version 2	866
RADIUS-Based EAP Protocols	866
RADIUS-Based EAP Authentication Flow	867
Extensible Authentication Protocol-Message Digest 5	867
Lightweight Extensible Authentication Protocol	868
Protected Extensible Authentication Protocol	868
Advantages of Using PEAP	868
Supported Supplicants for the PEAP Protocol	868
PEAP Protocol Flow	869
Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling	869
Benefits of EAP-FAST	869
EAP-FAST Flow	870

CHAPTER 33
Switch and Wireless LAN Controller Configuration Required to Support Cisco ISE

Functions	871
Enable Your Switch to Support Standard Web Authentication	872
Local Username and Password Definition for Synthetic RADIUS Transactions	872
NTP Server Configuration to Ensure Accurate Log and Accounting Timestamps	872
Command to Enable AAA Functions	872
RADIUS Server Configuration on the Switch	873
Configure the Switch to Send RADIUS Accounting Start/Stop to Inline Posture Nodes	874
Command to Enable RADIUS Change of Authorization (CoA)	874
Command to Enable Device Tracking and DHCP Snooping	874
Command to Enable 802.1X Port-Based Authentication	875
Command to Enable EAP for Critical Authentications	875
Command to Throttle AAA Requests Using Recovery Delay	875
VLAN Definitions Based on Enforcement States	875
Local (Default) ACLs Definition on the Switch	876
Enable Cisco Trustsec Switch Ports	878
Command to Enable EPM Logging	879

Command to Enable SNMP Traps	879
Command to Enable SNMP v3 Query for Profiling	879
Command to Enable MAC Notification Traps for Profiler to Collect	880
RADIUS Idle-Timeout Configuration on the Switch	880
Wireless LAN Controller Configuration for iOS Supplicant Provisioning	880
Wireless LAN Controller Support for Apple Devices	880
Configuring ACLs on the Wireless LAN Controller for MDM Interoperability	881

CHAPTER 34**Supported Management Information Bases in Cisco ISE 883**

IF-MIB	883
SNMPv2-MIB	884
IP-MIB	884
CISCO-CDP-MIB	885
CISCO-VTP-MIB	886
CISCO-STACK-MIB	886
BRIDGE-MIB	887
OLD-CISCO-INTERFACE-MIB	887
CISCO-LWAPP-AP-MIB	887
CISCO-LWAPP-DOT11-CLIENT-MIB	889
CISCO-AUTH-FRAMEWORK-MIB	890
EEE8021-PAE-MIB; RFC IEEE 802.1X	890
HOST-RESOURCES-MIB	890
LLDP-MIB	891



PART **I**

Introduction

- [Cisco ISE Features, page 3](#)
- [Navigate the Admin portal, page 11](#)



CHAPTER

1

Cisco ISE Features

- [Cisco ISE Features, page 4](#)
- [Key Functions, page 4](#)
- [Identity-Based Network Access, page 4](#)
- [Support for Multiple Deployment Scenarios, page 5](#)
- [Support for UCS Hardware, page 5](#)
- [Basic User Authentication and Authorization, page 5](#)
- [Policy Sets, page 6](#)
- [FIPS 140-2 Implementation, page 6](#)
- [Support for Common Access Card Functions, page 7](#)
- [Client Posture Assessment, page 7](#)
- [Network Access for Guests, page 8](#)
- [Support for Personal Devices, page 8](#)
- [Mobile Device Manager Interoperability with Cisco ISE, page 8](#)
- [Wireless and VPN Traffic with Inline Posture Nodes, page 8](#)
- [Profiled Endpoints on the Network, page 9](#)
- [Cisco pxGrid Services, page 9](#)
- [Cisco ISE Certificate Authority, page 9](#)
- [Support for Active Directory Multidomain Forests, page 9](#)
- [Support for SAnet Devices, page 9](#)
- [Support for Installation on Multiple Hardware and VMware Platforms, page 10](#)
- [Identity Provider as an External Identity Source, page 10](#)
- [Support for Automatic Failover for the Administration Node, page 10](#)

Cisco ISE Features

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 proactive 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.

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

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.

Cisco ISE platform can also be deployed as an Inline Posture node to perform policy enforcement and execute Change of Authorization (CoA) requests where users are accessing the network via WLCs and/or VPN concentrators that do not support the necessary functionality to facilitate Cisco ISE policy management.

Support for UCS Hardware

In addition to Cisco ISE 3300 Series appliance, Cisco ISE 1.4 supports the UCS C220 M3 hardware and is available on the following platforms:

- SNS-3415 (small)
- SNS-3495 (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 “AuthenticationStaus” 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.

Policy Sets

Cisco ISE supports policy sets, which let you group sets of authentication and authorization policies. As opposed to the basic authentication and authorization policy model, which is a flat list of authentication and authorization rules, policy sets let you logically define the organization’s IT business use cases into policy groups or services, such as VPN and 802.1x, such that it is easier for configuration, deployment, and troubleshooting.

You must enable Policy Sets on **Administration > System > Settings > Policy Settings** to make them available on the **Policy** menu.

FIPS 140-2 Implementation

Cisco ISE, supports Federal Information Processing Standard (FIPS) 140-2 Common Criteria EAL2 compliance. FIPS 140-2 is a United States government computer security standard that is used to accredit cryptographic modules. Cisco ISE uses an embedded FIPS 140-2 implementation using validated C3M and Cisco ACS NSS modules, per FIPS 140-2 Implementation Guidance section G.5 guidelines.

In addition, the FIPS standard places limitations on the use of certain algorithms, and in order to enforce this standard, you must enable FIPS operation in Cisco ISE. Cisco ISE enables FIPS 140-2 compliance via RADIUS Shared Secret and Key Management measures and provides SHA-256 encryption and decryption capabilities for certificates. While in FIPS mode, any attempt to perform functions using a non-FIPS compliant algorithm fails, and, as such, certain authentication functionality is disabled.

The certificates installed in ISE may need to be re-issued if the encryption method used in the certificates is not supported by FIPS. When you turn on FIPS mode in Cisco ISE, 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 a FIPS 140-2 compliant system and are disabled while Cisco ISE is in FIPS mode. Turning on FIPS mode also automatically disables PAP and CHAP protocols, which the Guest login function of Cisco ISE requires.

- Secure Shell (SSH) clients can only use SSHv2
- Lightweight Directory Access Protocol (LDAP) over Secure Sockets Layer (SSL)
- Inline Posture node RADIUS Key Wrap
- HTTPS protocol communication for both Administrator ISE nodes and Inline Posture nodes

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.

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.

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.

Wireless and VPN Traffic with Inline Posture Nodes

Inline Posture nodes are gatekeeping nodes that enforce Cisco ISE access policies and handle Change of Authorization (CoA) requests. After initial authentication (using EAP/802.1X and RADIUS), client machines must still go through posture assessment. The posture assessment process determines whether the client should be restricted, denied, or allowed full access to the network. When a client accesses the network through a WLC or VPN device, the Inline Posture node has the responsibility for the policy enforcement and CoA that

the other network devices are unable to accommodate. Consequently, a Cisco ISE can be deployed as an Inline Posture node behind other network access devices on your network, such as WLCs and VPN concentrators.

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.

Cisco pxGrid Services

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.

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.

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 Installation on Multiple Hardware and VMware Platforms

Cisco ISE comes preinstalled on a range of physical appliances with various performance characteristics. The Cisco Application Deployment Engine (ADE) and Cisco ISE software run either on a dedicated SNS-3400 Series appliance or on a virtual machine (Cisco ISE VM). The Cisco ISE software image does not support the installation of any other packages or applications on this dedicated platform. The inherent scalability of Cisco ISE allows you to add appliances to a deployment and increase performance and resiliency, as needed.

Identity Provider as an External Identity Source

Cisco ISE supports SAML Single Sign On (SSO) for the following portals:

- Guest portal (sponsored and self-registered)
- Sponsor portal
- My Devices portal

You can add an Identity Provider, such as Oracle Access Manager or Oracle Identity Federation, as an external identity source for a portal. The Identity Provider stores and validates the user credentials and generates a SAML response that allows the user to access the portal. It reduces password fatigue by removing the need for entering different user name and password combinations.

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 in Administration Nodes section in the Deploy Cisco ISE Nodes chapter for more information.



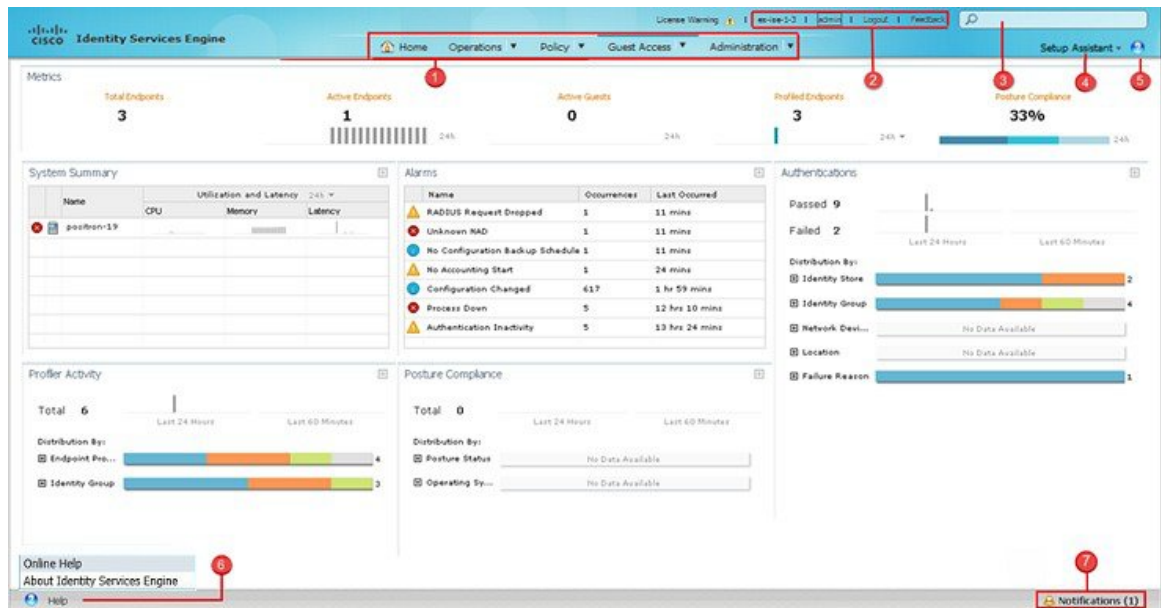
Navigate the Admin portal

- [Admin Portal, page 12](#)
- [Setup Assistant, page 14](#)
- [Filter Data on Listing Pages, page 18](#)
- [Cisco ISE Internationalization and Localization, page 20](#)
- [MAC Address Normalization, page 27](#)
- [Admin Features Limited by Role-Based Access Control Policies, page 27](#)

Admin Portal

The Admin portal is an administration console from which you can manage various identity services. The following figure shows the main elements of this portal.

Figure 1: Admin portal



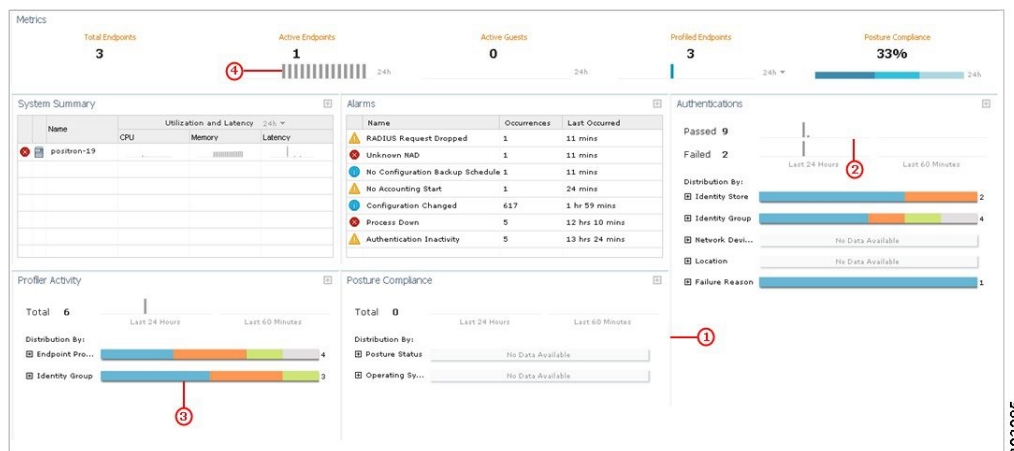
1	Menu Bar	<p>Access tools for viewing, monitoring, and managing different Cisco ISE options:</p> <ul style="list-style-type: none"> • Home: Access the dashboard, which is a real-time view of all the services running in the Cisco ISE network. • Operations: Access tools for monitoring real-time alarms and live authentications, querying historical data through reports, and troubleshooting network services. • 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 Panel	View the connected Cisco ISE node. Click the appropriate options to edit account information, log out, and provide feedback to Cisco.
3	Search	Search for endpoints and display their distribution by profiles, failures, identity stores, location, device type, and so on.
4	Setup Assistant	Access wizard to create a basic configuration to demonstrate Cisco ISE feature functionality in your network.

5	Context-Sensitive Help	Access help for the currently displayed page.
6	Help	Access the complete Cisco ISE online Help system.
7	Notifications	Hover the mouse cursor over this option to view a summary of notifications.

Cisco ISE Dashboard

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.

Figure 2: Cisco ISE User Dashboard



303285

1	Dashlets	<p>Dashboard element that displays statistical summaries about the devices and user accessing the network. In some dashlets, colored icons are displayed prior to the device names to convey the system health:</p> <ul style="list-style-type: none"> • Green = Healthy • Yellow = Warning • Red = Critical • Gray = No information
2	Sparklines	Depict trends over time.
3	Stacked bar charts	Display the distribution of parameters using color as the dividing element, so you can see where one parameter ends and another begins. Display is limited to the top 10 distributions. In general, stacked bar charts use color to mark the boundary points between one data measurement and another.

4	Metric meters	Summarize the most important statistics regarding the devices that are accessing the network. Metric meters provide an at-a-glance view of network health and performance. You can click the number displayed above the metrics meter to view more information about the devices.
---	---------------	---

Setup Assistant

The Setup Assistant guides you through a series of questions in a wizard-like interface retaining your responses and using them to configure Cisco ISE directly. It enables you to set up a basic working Cisco ISE configuration as a proof-of-concept for your network. Your answers to the questions impact these Cisco ISE features: authentication, authorization, profiling, posture, client provisioning, guest services, and support for personal devices.

Cisco ISE Licensing Impact on Setup Assistant

Setup Assistant functionality depends on the Cisco ISE license that you have applied to your configuration.

Cisco ISE License	Identify Policy Requirements	Configure Network Access Services	Select Network Device Types
Basic	—	The posture, endpoint profiling, and personal devices options are not available.	—
Advanced	If you choose wired + monitor, the guest and posture choices are disabled on the next page. If you choose wireless and wired + monitor, the guest and posture choices on the next page impact wireless only.	The guest and posture choices are not available if you select wired + monitor on the previous page.	If you choose wired only on the first page, the wireless LAN controller (WLC) information does not appear. If you choose wireless only on the first page, switch information does not appear.
Wireless	The wired option is not available.	—	Switch information does not appear.

Run the Setup Assistant

When you start Cisco ISE for the first time, you are prompted to run the Setup Assistant. If you choose not to run it then, you can run it again later.

Before You Begin

To perform this task, you must be a Super Admin. You can only run the Setup Assistant on the standalone or Primary Administration Node (PAN).

Step 1 Click **Setup Assistant** in the upper-right corner of the Admin portal.

Step 2 Follow the on-screen instructions to complete the configuration.

Setup Assistant Overwrites Previous Configurations

Each time you run the Setup Assistant, Cisco ISE overwrites previous settings, which can critically impact your configuration in the following ways:

- All authentication, authorization, client provisioning, and posture policies are deleted and replaced, including any that you added without using the Setup Assistant.
- Other settings, such as policy elements and web portal customizations, are overwritten with any newly specified values. If you do not enter anything for the optional settings, the Setup Assistant resets them to their default values.

Identify Policy Requirements Page in Setup Assistant

Wired or Wireless

You must indicate whether you want to support wired or wireless connections, or both. If you are using a Cisco ISE Wireless License, the wired option is unavailable.

These choices impact the policies that Cisco ISE creates, and also dictate other required responses. For example, if you choose wired, you can also indicate whether your network supports IP phones.

You must also indicate whether or not the wired connections are monitored or if network access must be enforced based on compliance:

- Monitor generates non-compliance logs and reports, but does not require that users or devices comply with the defined policies.

In monitoring mode, posture and guest policies are ignored. If you support wired connections in monitoring mode, the Setup Assistant disables the guest and posture choices on the next page to prevent unauthorized computer and guest access.

If you support wired and wireless connections, you can enable the guest and posture features, but they will apply only to the wireless connections. The wireless connections always runs in enforcement mode.

- Enforce requires compliance with the defined policies.

Protected Subnets

You must indicate which subnets should be inaccessible by guests or noncompliant endpoints. This information is used when creating the downloadable ACLs.

Configure Network Access Service Page in Setup Assistant

User Authentication

Users belonging to these groups will be granted network access as employees and be allowed to create guest accounts using the Sponsor portal.

- **Internal users**—If you choose to create an internal user, Cisco ISE creates a single user using the name you enter and assigns the user to the default Employee and ALL_ACCOUNTS user identity groups. You can verify this in the **Administration > Identity Management > Identities > Users** page after setup completes.

Because the Setup Assistant provides only the basic Cisco ISE configuration to demonstrate its functionality in your network, you cannot use it to import additional users into the internal user database. You can add additional internal users using the Admin portal after you complete the Setup Assistant.

- **Active Directory**—If you choose to join the Active Directory domain, Cisco ISE adds the indicated AD domain and joins to it. After joining the domain, you must choose an Active Directory group. All users belonging to this group will be able to authenticate using Dot1x and create guests using the Sponsor portal. You can verify this from the **Administration > Identity Management > External Identity Sources > Active Directory** page after setup completes.

Posture Compliance

When you enable posture using the Setup Assistant, Cisco ISE checks for antispyware and antivirus definitions and installations on connected endpoints.

You must indicate whether you want to assess or assess and enforce posture compliance for employees and guests:

- **Assess** generates reports about noncompliant users, but allows them to be authenticated.
- **Enforce** prevents authentication.

If you want to force Cisco ISE to redirect noncompliant endpoints to a remediation server before granting network access, enter the proxy server IP address.

If you enable posture compliance, Cisco ISE will:

- Download the Cisco NAC agents and update the **Policy > Policy Elements > Results > Client Provisioning > Resources** page.
- Create the downloadable ACLs on the **Policy > Policy Elements > Results > Authorization > Downloadable ACLs** page. All DACLs created by the Setup Assistant include the prefix AutoGen, such as: AutoGen_DACL_PrePostureWired.
- Create authorization profiles on the **Policy > Policy Elements > Results > Authorization > Authorization Profiles** page. Authorization profiles created by the Setup Assistant include the prefix AutoGen, such as: AutoGen_profile_Byod_CWA.
- Create authorization conditions on the **Policy > Policy Elements > Conditions > Authorization > Simple Conditions** and **Policy > Policy Elements > Conditions > Authorization > Compound Conditions** pages. Authorization conditions created by the Setup Assistant include the prefix AutoGen, such as: AutoGen_condition_Android_Devices or AutoGen_condition_GuestWired.

- Create client provisioning policies on the **Policy > Client Provisioning** page. Client provisioning policies created by the Setup Assistant include the prefix AutoGen, such as: AutoGen_Provisioning.
- Download posture updates from the **Administration > System > Settings > Posture > Updates** page.
- Create posture policies on the **Policy > Posture** page. Posture policies created by the Setup Assistant include the prefix AutoGen, such as: AutoGen_Policy_Check_For_AS_Definition_Mac_Employee.
- Create authorization policies on the **Policy > Authorization** page. Authorization policies created by the Setup Assistant include the prefix AutoGen, such as: AutoGen_policy_Registered_Wireless_Devices.
- Create authentication policies on the **Policy > Authentication** page. Authorization policies created by the Setup Assistant include the prefix AutoGen, such as: AutoGen_AuthNPolicy_MAB.

Endpoint Profiling

Endpoint profiling discovers, identifies, and determines the capabilities of all attached endpoints on your network. If you enable endpoint profiling, Cisco ISE will:

- Enable these endpoint profiling features on the **Administration > System > Deployment > Edit Node > Profiling Configuration** page.
 - DHCP
 - RADIUS
 - Network Scan (NMAP)
 - SNMP Query Probes
- Configure SNMP on the **Administration > Network Resources > Network Devices** page.

Proxy Settings

Cisco ISE uses the proxy server to download Cisco-defined posture checks and client provisioning resources required for assessing posture of endpoints and allowing personal devices on the network. If you configure these proxy settings, Cisco ISE will update the settings on the **Administration > System > Settings > Proxy** page.

Guest User Support

To support guest users, you must create a sponsor user. Cisco ISE creates a single user using the name you enter and assigns the user to the default ALL_ACCOUNTS user identity group, which defines the user as a sponsor user. You can verify this from the **Administration > Identity Management > Identities > Users** page after setup completes.

If you add a simplified URL, Cisco ISE updates the **Portal Name** settings at the top of the **Guest Access > Configure > Sponsor Portals > Edit** page.

Support for Personal Devices

You can add a simplified URL for employees to use to access the My Devices portal, and Cisco ISE updates the **Portal Name** settings at the top of the **Administration > Device Portal Management > My Devices > Edit** page.

Web Portal Customizations

You can upload an image to use as a custom logo for the Sponsor, Guest, and My Devices portals. Cisco ISE also will upload the image to the appropriate page:

- Guest portals: **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
- Sponsor portals: **Guest Access > Configure > Sponsor Portals > Edit > Portal Page Customization**
- **Administration > Device Portal Management > My Devices > Edit > Portal Page Customization**

Select Network Device Types Page in Setup Assistant

Switches and Wireless Controllers

Cisco ISE adds the switches and wireless controllers to the **Administration > Network Resources > Network Devices** page, updates the SNMP settings, and adds the RADIUS shared secret to the Authentication Settings option.

Depending on the choices you made previously, you must configure the switches and wireless controllers. Click the **Wired** or **Wireless Network Diagram** links to display sample network topologies that illustrate the required configuration details.

Review and Confirm Your Choices Page in Setup Assistant

Review Your Selection

You can verify your responses to each of the questions.

Network Device Configuration

Configuration details for each configured switch and WLC display separately. Cisco ISE does not automatically update these configurations on the devices. If you want to completely replace the current device configuration, copy and paste the entire configuration. Alternatively, you can just copy the specific sections with the configuration changes you need. You can access the most current copy of the settings after exiting the Setup Assistant by choosing **Setup Assistant > View network device configuration**.

ISE Configuration

The ISE Configuration tab displays details about each setting, policy, profile, DACL, and network device added to Cisco ISE.

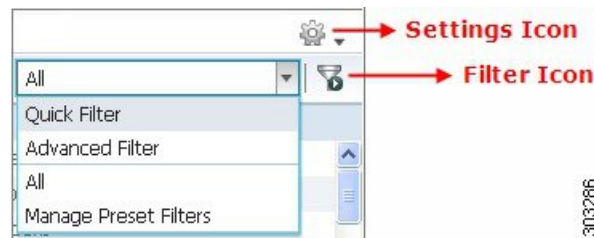
Filter Data on Listing Pages

Listing pages include tools that enable you to filter and customize the displayed information.

Data Filters in Listing Pages

You can customize and filter the information that displays in the listing pages using the settings and filter icons.

Figure 3: Data Filters Example



Customize the Displayed Field Attributes

You can customize the field attributes displayed in the listing pages. The available and default options vary based on the specific listing page.

-
- Step 1** Click the Settings icon and choose **Columns**.
 - Step 2** Select the items to add or remove. A checkmark displays next to the selected items.
 - Step 3** Click **Close**.
-

Filter Data by Field Attributes Using the Quick Filter

The Quick Filter allows you to enter a value for any of the field attributes displayed in the listing page, refreshes the page, and lists only those records that match your filter criteria.

-
- Step 1** Click the **Show** drop-down list and choose **Quick Filter**.
 - Step 2** Enter search criteria in one or more of the attribute fields, and the entries that match the specified attributes display automatically.
-

Filter Data by Conditions Using the Advanced Filter

The Advanced Filter allows you to filter information based on specified conditions, such as, First Name = Mike and User Group = Employee. You can specify more than one condition.

-
- Step 1** Click the **Show** drop-down list and choose **Advanced Filter**.
 - Step 2** Specify search the search attributes, such as fields, operators, and values from the Filter menus.
 - Step 3** Click + to add additional conditions.
 - Step 4** Click **Go** to display the entries that match the specified attributes.
-

Create Custom Filters

You can create and save custom filters and modify the filter criteria in preset filters. Custom filters are not saved in the Cisco ISE database. You can only access them using the same computer and browser used to create them.

-
- Step 1** Click the **Show** drop-down list and choose **Advanced Filter**.
 - Step 2** Specify the search attributes, such as fields, operators, and values from the Filter menus.
 - Step 3** Click + to add additional conditions.
 - Step 4** Click **Go** to display the entries that match the specified attributes.
 - Step 5** Click the **Save** icon to save the filter.
 - Step 6** Enter a name and click **Save**. The filter now appears in the Show drop-down list.
-

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.

In Cisco ISE, internationalization 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 internationalization support for the following languages and browser locales:

Language	Browser Locale
Chinese traditional	zh-tw

Language	Browser Locale
Chinese simplified	zh-cn
Czech	cs-cz
Dutch	nl-nl
English	en
French	fr-fr
German	de-de
Hungarian	hu-hu
Italian	it-it
Japanese	ja-jp
Korean	ko-kr
Polish	pl-pl
Portuguese (Brazil)	pt-br
Russian	ru-ru
Spanish	es-es

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 user name 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. If you are experiencing difficulties with a Windows native supplicant, the following Windows hotfixes may be helpful:

- <http://support.microsoft.com/default.aspx?scid=kb;EN-US;957218>
- <http://support.microsoft.com/default.aspx?scid=kb;EN-US;957424>



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 1.2, 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.

Cisco NAC and MAC Agent UTF-8 Support

The Cisco NAC agent supports internationalization of text, messages, and any UTF-8 data that is exchanged with Cisco ISE. This includes requirement messages, requirement names, and file and process names that are used in conditions.

The following limitations apply:

- UTF-8 support applies to Windows-based NAC agents only.
- Cisco NAC and MAC agent interfaces currently do not support localization.

- WebAgent does not support UTF-8 based rules and requirements.
- If an acceptable use policy (AUP) is configured, the policy pages are provided on the client side, based on the browser locale and the set of languages that are specified in the configuration. You are responsible for providing a localized AUP bundle or site URL.

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 administrator passwords with UTF-8 characters.
- Cisco ISE does not support UTF-8 characters in certificates.

Table 1: Admin Portal UTF-8 Character Fields

Admin Portal Element	UTF-8 Fields
Network access user configuration	<ul style="list-style-type: none"> • User name • First name • Last name • e-mail
User list	<ul style="list-style-type: none"> • All filter fields • Values shown on the User List page • Values shown on the left navigation quick view
User password policy	<ul style="list-style-type: none"> • Advanced > Password may not contain characters <p>Some languages do not have uppercase or lower case 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:</p> <ul style="list-style-type: none"> • Lowercase alphabetic characters • Uppercase alphabetic characters
Administrator list	<ul style="list-style-type: none"> • All filter fields • Values shown on the Administrator List page • Values shown on the left navigation quick view
Admin login page	<ul style="list-style-type: none"> • User name
RSA	<ul style="list-style-type: none"> • Messages • Prompts
RADIUS token	<ul style="list-style-type: none"> • Authentication tab > Prompt

Admin Portal Element	UTF-8 Fields
Posture Requirement	<ul style="list-style-type: none"> • Name • Remediation action > Message shown to Agent User • Requirement list display
Posture conditions	<ul style="list-style-type: none"> • File condition > File path • Application condition > Process name • Service condition > Service name • Conditions list display
Guest and My Devices settings	<ul style="list-style-type: none"> • Sponsor > Language Template: all supported languages, all fields • Guest > Language Template: all supported languages, all fields • My Devices > Language Template: all supported languages, all fields
System settings	<ul style="list-style-type: none"> • SMTP Server > Default e-mail address
Operations > Alarms > Rule	<ul style="list-style-type: none"> • Criteria > User • Notification > e-mail Notification user list
Operations > Reports	<ul style="list-style-type: none"> • Operations > Live Authentications > Filter fields • Operations > Reports > Catalog > Report filter fields
Operations > Troubleshoot	<ul style="list-style-type: none"> • General Tools > RADIUS Authentication Troubleshooting > Username
Policies	<ul style="list-style-type: none"> • Authentication > value for the av expression within policy conditions • Authorization / posture / client provisioning > other conditions > value for the av expression within policy conditions

Admin Portal Element	UTF-8 Fields
Attribute value in policy library conditions	<ul style="list-style-type: none"> • Authentication > simple condition / compound condition > value for the av expression • Authentication > simple condition list display • Authentication > simple condition list > left navigation quick view display • Authorization > simple condition / compound condition > value for the av expression • Authorization > simple condition list > left navigation quick view display • Posture > Dictionary simple condition / Dictionary compound condition > value for the av expression • Guest > simple condition / compound condition > value for the av expression

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.

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 > Authorization
- 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 '.')

- 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. Read-only functionality is unavailable for any administrative access.



PART **II**

Deploy Cisco ISE Nodes

- [Set Up Cisco ISE in a Distributed Environment, page 31](#)
- [Set Up Inline Posture, page 71](#)



Set Up Cisco ISE in a Distributed Environment

- [Cisco ISE Distributed Deployment, page 32](#)
- [Cisco ISE Deployment Terminology, page 32](#)
- [Personas in Distributed Cisco ISE Deployments, page 32](#)
- [Administration Node, page 33](#)
- [Policy Service Node, page 39](#)
- [Monitoring Node, page 40](#)
- [Cisco pxGrid Services, page 42](#)
- [Cisco pxGrid Live Logs, page 43](#)
- [ISE pxGrid Identity Mapping, page 43](#)
- [Inline Posture Node, page 56](#)
- [Cisco ISE Distributed Deployment, page 57](#)
- [Configure a Cisco ISE Node, page 60](#)
- [Register an Inline Posture Node, page 63](#)
- [View Nodes in a Deployment, page 64](#)
- [Synchronize Primary and Secondary Cisco ISE Nodes, page 64](#)
- [Create a Policy Service Node Group, page 64](#)
- [Deploy Cisco pxGrid Services, page 65](#)
- [Change Node Personas and Services, page 66](#)
- [Manually Promote Secondary Administration Node To Primary, page 66](#)
- [Configure Primary Administration Node for Automatic Failover, page 67](#)
- [Configure Monitoring Nodes for Automatic Failover, page 68](#)
- [Remove a Node from Deployment, page 69](#)
- [Change the Hostname or IP Address of a Standalone Cisco ISE Node, page 69](#)
- [Replace the Cisco ISE Appliance Hardware, page 70](#)

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. The Inline Posture node cannot assume any other persona, due to its specialized nature. The Inline Posture node must be a dedicated node.

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, pxGrid, and Inline Posture. The Inline Posture persona requires a dedicated Cisco ISE node. 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, Monitoring, or Inline Posture personas.

A Cisco ISE node can provide various services based on the persona that it assumes. Each node in a deployment, with the exception of the Inline Posture node, 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
- A pair of Inline Posture nodes for high availability

You need to add Canonical Name (CNAME) record of the ISE hostname to the DNS. Ensure that you create CNAME RR along with the A record for each Cisco ISE node. If CNAME record is not created, it might result in the alarm 'DNS Resolution failed for CNAME <hostname of the node>'.

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 in Administration Nodes

In a high-availability configuration, the PAN is in the active state to which all configuration changes are made. The Secondary Administration Node is in the standby state, and will receive all configuration updates from the PAN. Therefore, it will always have a complete copy of the configuration from the PAN.

If the PAN goes down, you must log in to the user interface of the Secondary Administration Node and manually promote the Secondary Administration Node. There is no automatic failover for the Administration persona.

When the PAN is down, sponsors cannot create new guest accounts. During this time, guest and sponsor portals will provide read-only access to already created guests and sponsors, respectively. Also, a sponsor who has never logged in to the sponsor portal before the PAN goes offline, will not be able to log in to the sponsor portal until a Secondary Administration Node is promoted or the PAN becomes available.

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

The following table lists a set of features and specifies whether they are available or not when the PAN goes down.

Feature	Available When the PAN Goes Down(Yes/No)
Existing internal user RADIUS authentication	Yes
Existing or New AD user RADIUS authentication	Yes
Existing endpoint with no profile change	Yes
Existing endpoint with profile change	Yes
New endpoint learned through profiling	Yes
Existing guest – LWA	Yes
Existing guest – CWA	Yes
Guest change password	No (Guest must log in with old password)
Guest – AUP	Yes
Guest – Max Failed Login Enforcement	No
New Guest (Sponsored or Self-registered)	No

Feature	Available When the PAN Goes Down(Yes/No)
Posture	Yes
New Device Registration	No
Existing Registered Devices	Yes
pxGrid Service	No

In a high availability configuration, the PAN is in the active state to which all configuration changes are made. The Secondary Administration Node is in the standby state, and will receive all configuration updates from the PAN. Therefore, it will always have a complete copy of the configuration from the PAN.

Cisco ISE supports automatic failover for the Administration persona. If the 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 in the configured interval called the 'Polling Interval'. If the health check response received for the PAN health is down or unreachable, the health check node initiates the promotion of the Secondary Administration Node to take over the primary role after waiting for configured threshold value of 'Count of failures before failover'.

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.

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

Features	Available When PAN is Down (Yes/No)
Existing internal user RADIUS authentication	Yes
Existing or New AD user RADIUS authentication	Yes
Existing endpoint with no profile change	Yes
Existing endpoint with profile change	No
New endpoint learned through profiling	No
Existing guest – LWA	Yes
Existing guest – CWA	Yes (apart from flows enabled for device registration, such as Hotspot, BYOD, and CWA with automatic device registration)
Guest change password	No
Guest – AUP	No
Guest – Max Failed Login Enforcement	No

Features	Available When PAN is Down (Yes/No)
New Guest (Sponsored or Self-registered)	No
Posture	Yes
BYOD with Internal CA	No
Existing Registered Devices	Yes
MDM On-boarding	No
pxGrid Service	No

For certificate provisioning with the internal certificate authority, you have to import the root certificate of the original PAN and its key in to the new primary node, after promotion. Certificate provisioning will not work post auto-failover from PSN nodes that are newly added, that is, added after the promotion of the secondary node to PAN.

High-Availability Health Check Nodes

Health check node for PAN is called active health check node whereas health check node for Secondary Administration Node is called passive health check node. Active health check node is responsible for checking status of PAN and managing the automatic failover of Administration nodes. It is recommended to have two non-administration ISE nodes designated as the health check nodes, one each for the primary and Secondary Administration Nodes. You can also designate a single non-administration ISE node as the health check node for both the PAN and the Secondary Administration Node. In case a single health check node is checking the health of both the PAN and the Secondary Administration Node, it assumes both the active and passive roles.

A health check node is a non-administration node and can be a Policy Service, Monitoring, or pxGrid node, or a combination of these. It is recommended that PSN nodes that are in the same data center as the Administration nodes, are designated as high-availability health check nodes. However, in a small or a centralized deployment where the two Administration nodes are in the same location (LAN or data center), any node (PSN/pxGrid/MnT) not having the Administration persona can be used as high-availability health check node.

Health Probe by Health Check Nodes

The health check node for the PAN reaches out for its health status, for the configured polling intervals. If the health status of the PAN is down or unreachable for the configured 'Number of failure polls before failover' value, the primary health check node notifies the Secondary Administration Node to take over as the PAN of the deployment.

The health check node for automatic failover is the single point of failure. If the health check node for the PAN itself goes down, high-availability failover will not happen.

Startup of Health Check Node

The health check node for the Secondary Administration Node is a passive monitor. It does not take any action until the Secondary Administration Node has been promoted as the PAN. When the Secondary Administration

Node 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 PAN becomes the health check node for the Secondary Administration Node now and would monitor it passively.

Shutdown of Health Check Node

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 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.

Restart of Health Check Node

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

Health Check of the Primary Administration Node

The active health check node checks the health status of the Primary Administration Node (PAN) at a configured polling interval. It sends a request to the PAN, and if the response that it receives satisfies the specified configuration, then the health check node considers the PAN to be in good health. Otherwise, the health check node considers the PAN to be in bad health. If the health of the PAN is bad continuously for more than the configured 'Number of Failure Polls before Failover' value, health check node initiates failover to the Secondary Administration Node.

If at any time during the health check, health status is found to be good after being reported as bad previously within the 'Number of Failure Polls before Failover' value, health check node marks the PAN status as good and resets the health check cycle.

Response from health check of the 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 Administration Node.

For example, assume that the health check node (N1) goes out-of-sync and some other node (N2) is made the health check node of the PAN. In such a case, once the PAN goes down, there is no way for N1 to know that there is another node (N2) checking the same PAN. Later, if N2 too goes down or out of network, an actual failover would be required. The Secondary Administration Node, however, retains the right to reject the promotion request. So, once the Secondary Administration Node has been promoted to the primary role, further promotion request (from the node checking node N2) would be rejected with an error. Even if the high-availability health check node for PAN is out of sync, it continues to check the health of PAN. If the health check response is valid for failover (that is, response says that the correct PAN is checked by the correct health check node and health check node has the correct Secondary Administration Node information), it would also attempt to failover to the Secondary Administration Node when the PAN meets the failover criteria.

Automatic Failover of the Secondary Administration Node

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

- Whether the PAN is available in network.

- Whether failover request came from a valid health check node.
- Whether failover request was received by a wrong node.

If all the validations pass, secondary Administration node promotes itself to the primary role.

The following are some sample (but not limited to) scenarios where automatic failover of the secondary Administration node would be attempted.

- Health of PAN is consistently not good for the 'Number of failure polls before failover' value during the polling period.
- Cisco ISE services on the PAN is manually stopped and remains so for the configured 'Number of Failure Polls before Failover' value.
- PAN is shut down using soft halt or reboot option and remains shut for the configured 'Number of Failure Polls before Failover' value.
- PAN goes down abruptly (power down) and remains down for the configured 'Number of Failure Polls before Failover' value.
- Network interface of 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 so for the configured 'Number of Failure Polls before Failover' value.

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 PAN information.
- Promotion request is received from an incorrect health check node.
- Promotion request is received but the PAN is up and in good health.
- Node receiving the promotion request goes out-of-sync.

Fallback to the Original PAN

Cisco ISE does not support fallback to original PAN. This means that after the automatic failover to the Secondary Administration Node is initiated, if the original PAN is brought back into the network, the original primary node would continue to have the secondary role and would not be promoted back to the primary role.

Manual Promotion of the Secondary Administration Node

Cisco ISE supports both automatic and manual promotion of secondary Administration node to the primary role. When auto-failover is enabled, you can still perform manual promotion of the secondary Administration node. Promotion of the secondary Administration node to primary role is fairly independent and is not affected whether the promotion is performed manually or automatically.

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.

Functionality	Affect Details
Operations that are Blocked	
Upgrade	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. You must have at least two Administrative nodes and one non-Administrative node in your deployment to enable PAN auto-failover.
Restore of Backup	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.
Change Node Persona	Change of the following node personas via the user interface will be blocked: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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

Functionality	Affect Details
Other Administration Portal Operations	<p>The following admin operations via the user interface will be blocked:</p> <ul style="list-style-type: none"> • Patch Installation and Roll back • Change HTTPS certificate. • Change admin authentication type from password-based authentication to certificate-based authentication and viceversa.
Operations that Require PAN Auto-Failover to be Disabled	
CLI Operations	<p>The following admin operations via the CLI will display a warning message if PAN auto-failover configuration is enabled. These operations may trigger auto-failover if service/system is not restarted within failover window. Hence, while performing the below operations it is recommended to disable PAN auto-failover configuration:</p> <ul style="list-style-type: none"> • Manual ISE service stop • Soft reload (reboot) using admin CLI

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-redirectioned 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-redirectioned 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-redirectioned 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 64 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-redirectioned 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-redirectioned 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.

You can have a maximum of 10 Policy Service nodes 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 and the Primary Monitoring Node 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 primary Monitoring node. 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.

Cisco pxGrid Services

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 an endpoint profile meta topic. Cisco pxGrid also supports bulk download of tags and endpoint profiles.

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.

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. You can enable or disable capabilities. If disabled, the client is unsubscribed. Capability information is available from the publisher through publish, directed query, or bulk download query.

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 Identity Mapping. For more information, see [Configure Identity Mapping](#), on page 44.

-
- Step 1** Choose **Administration > pxGrid Services**.
- Step 2** Check the checkbox next to the client and click **Approve**.
- Step 3** To view the capabilities, click **View by Capabilities** at the top-right.
- 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.

ISE pxGrid Identity Mapping

Identity Mapping 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, it is possible to use Identity Mapping to collect user authentication information from the active directory (AD) Domain Controller. The Identity Mapping connects to Windows system using the MS WMI interface and queries logs from the Windows event messaging. Once a user logs into the network and is authenticated with an Active Directory, the Domain Controller generates an event log that includes the user name and IP address allocated for the user.

Identity mapping can also be activated even if Cisco ISE plays an active role for authentication. In such cases, the same session may be identified twice. The operational data has a session attribute that indicates the source. You can go to Operations > Authentications and click **Show Live Sessions** to check the Session Source.

The Identity Mapping component retrieves the user logins from the Domain Controller and imports them into the Cisco ISE session directory. So 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, and the AD DC host name and the AD DC NetBios name.

The Cisco ISE plays only a passive role and does not perform the authentication. When Identity Mapping is active, Cisco ISE collects the login information from the AD and includes the data into the session directory.

Key Features

- Identity Mapping is configured from the Cisco ISE administration console. The configuration includes the following settings:
 - Definition of all the DCs from which Identity Mapping is to collect user authentication information. This also includes import and export of the DC list using *.csv files
 - DC connection characteristics such as authentication security protocol (NTLMv1 or NTLMv2) and user session aging time
 - Connection testing, to verify the DC is set correctly to initialize valid connection with Identity Mapping
- Identity Mapping report. This report provides information about the Identity Mapping component for troubleshooting
- Identity Mapping debug logs
- Cisco ISE session directory maintains the collected user information, so that customers can view it from the Live Sessions and query it from the pxGrid interface
- Using the CLI command **show application status** provides the health status of nodes that use Identity Mapping
- Supports High Availability

Configuring Identity Mapping

ID Mapping requires configuration in ISE, and the Active Directory Domain Server must have the right patches and configuration. For information about configuring the Active Directory domain controller for ISE, see [Active Directory Requirements to Support Identity Mapping](#), on page 46

Configure Identity Mapping

ISE must be able to establish a connection with an AD Domain Controller (DC).

Before You Begin

Enable pxGrid services to configure Identity Mapping. Choose **Administration > System > Deployment** to enable pxGrid services.

To add a new Domain Controller (DC) for Identity Mapping, you need the login credentials of that DC.

Make sure the Domain Controller is properly configured for ISE Identity Mapping, as described in [Active Directory Requirements to Support Identity Mapping](#), on page 46.

-
- Step 1** Choose **Administration > pxGrid Identity Mapping > AD Domain Controller**.
- Step 2** Click **General Settings**.
- Step 3** The Active Directory General Settings pop-up is displayed. Set the required values and click **Save**.
- **History interval** is the time during which Identity Mapping reads user login information that already occurred. This is required upon startup or restart of Identity Mapping to catch up with events generated while it was unavailable.
 - **User session aging time** is the amount of time the user can be logged in. Identity Mapping 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.
 - You can select either **NTLMv1** or **NTLMv2** as the communications protocol between the ISE and the DC.
- Step 4** Click **Add**.
- Step 5** In the **General Settings** section, enter the **Display Name**, **Domain FQDN**, and **Host FQDN** of the DC.
- Step 6** In the **Credentials** section, enter the Username and Password of the DC.
- Step 7** (Optional) Test the connection to the specified domain by clicking **Verify DC Connection Settings**. This test ensures that the connection to the DC is healthy. However it does not check whether Cisco ISE can fetch the user information upon login.
- Step 8** Click **Submit**. An updated table is displayed with the newly-defined DC included in the list of DCs. The status column indicates the different states of DC. You can also Import or Export the DC list.
- Note** While importing, you need to provide the password in the template. As the file contains password, the import template should be treated as sensitive. The Export option does not export the password.
-

Filter Identity Mapping

You can filter certain users, based on their name or IP address. 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. The Monitoring live session shows Identity Mapping components that are not filtered out by the Mapping Filters.

-
- Step 1** Choose **Administration > pxGrid Identity Mapping > Mapping Filters**.
- Step 2** Click **Add**, enter the Username and or IP address of the user you want to filter and click **Submit**.
- Step 3** To view the non-filtered users that are currently logged into the Monitoring session directory, choose **Operations > Authentications**.
-

Active Directory Requirements to Support Identity Mapping

Identity Mapping uses 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 logins information. The following sections show how configure the Active Directory domain controller to support ISE Identity Mapping .

Configure Active Directory for Identity Mapping

ISE Identity Mapping uses 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>

This patch fixes a memory leak in Microsoft's WMI, which prevents CDA to establish successful connection with the domain controller (CDA administrator can experience it in CDA Active Directory domain controller GUI page, where the status need to be "up" once the connection establishes successfully).

- <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 CDA 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>

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 CDA may not get all user login events from this domain controller.

- <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>

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.

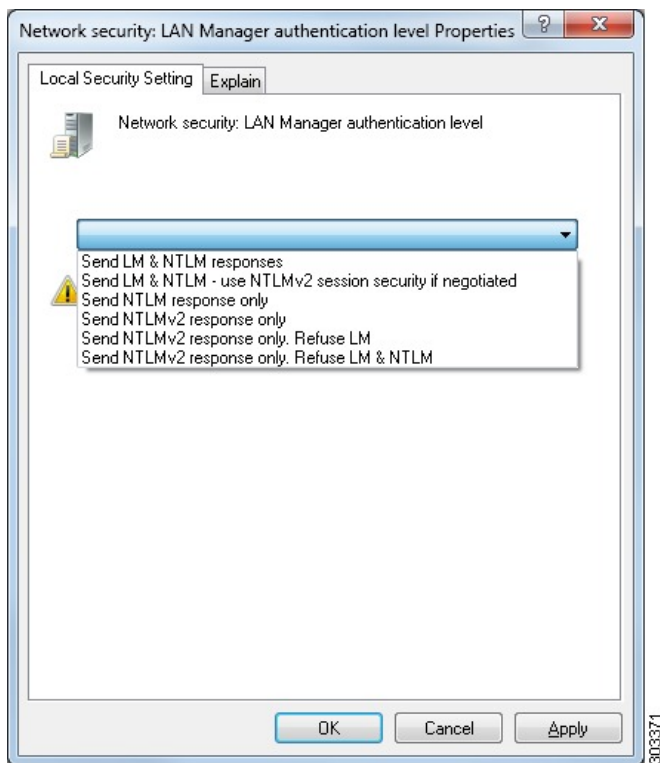
Step 3 You must have an Active Directory user with sufficient permissions for ISE to connect to the Active Directory. The following instructions show how to define permissions either for admin domain group user or none admin domain group user:

- 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 2: Supported Authentication Types Based on ISE and AD NTLM Version Settings

ISE NTLM setting options / Active Directory (AD) NTLM setting options NTLMv1 NTLMv2	NTLMv1	NTLMv2
Send LM & NTLM responses connection is allowed connection is allowed	connection is allowed	connection is allowed
Send LM & NTLM - use NTLMv2 session security if negotiated connection is allowed connection is allowed	connection is allowed	connection is allowed
Send NTLM response only connection is allowed connection is allowed	connection is allowed	connection is allowed
Send NTLMv2 response only connection is allowed connection is allowed	connection is allowed	connection is allowed
Send NTLMv2 response only. Refuse LM connection is allowed connection is allowed	connection is allowed	connection is allowed
Send NTLMv2 response only. Refuse LM & NTLM connection is refused connection is allowed	connection is refused	connection is allowed

Figure 4: MS NTLM Authentication Type Options**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.
- Step 4** Choose **Default Domain Controllers Policy > Computer Configuration > Policies > Windows Settings > Security Settings**.
- 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 52](#)
- [Set Permissions for Access to WMI Root/CIMv2 Name Space, on page 54](#)
- [Grant Access to the Security Event Log on the AD Domain Controller, on page 55](#)

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

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 ID Mapping 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 5: Local and Remote Access for Access Permissions

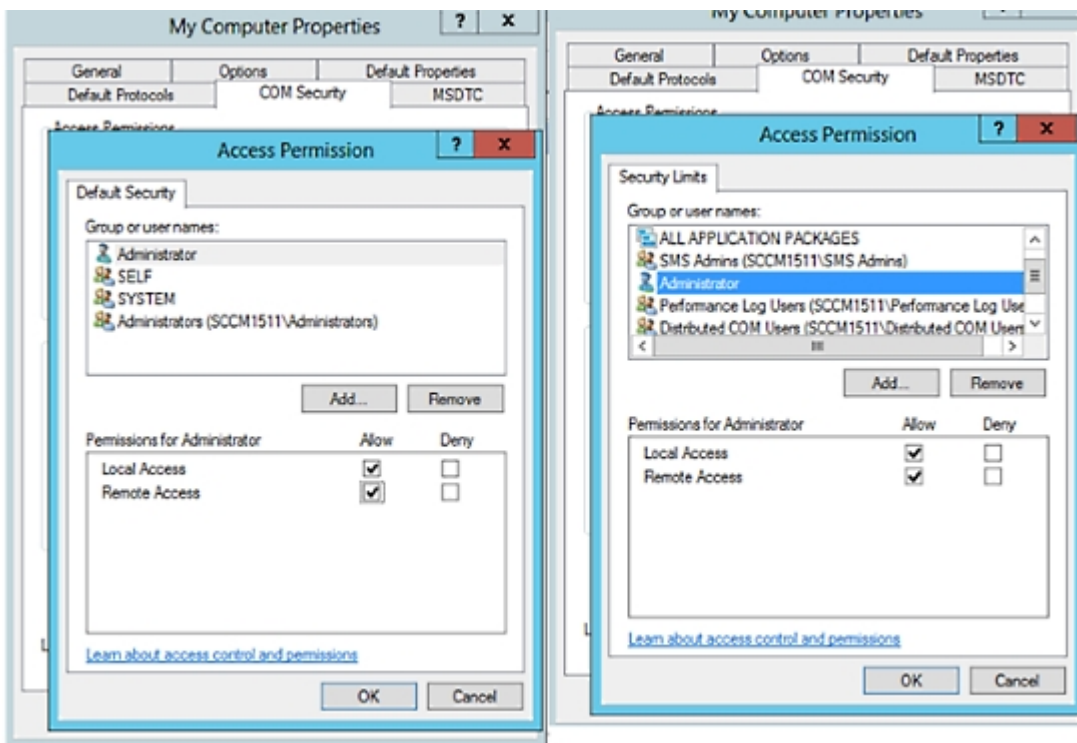
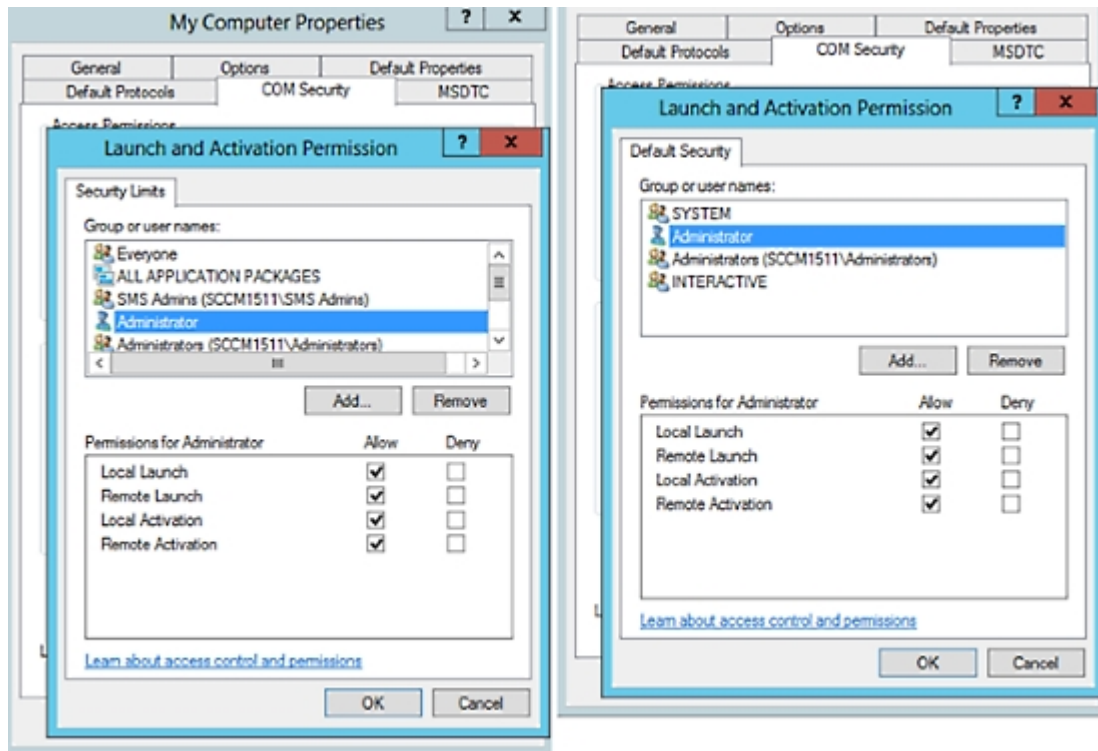


Figure 6: Local and Remote Access for Launch and Activation Permissions

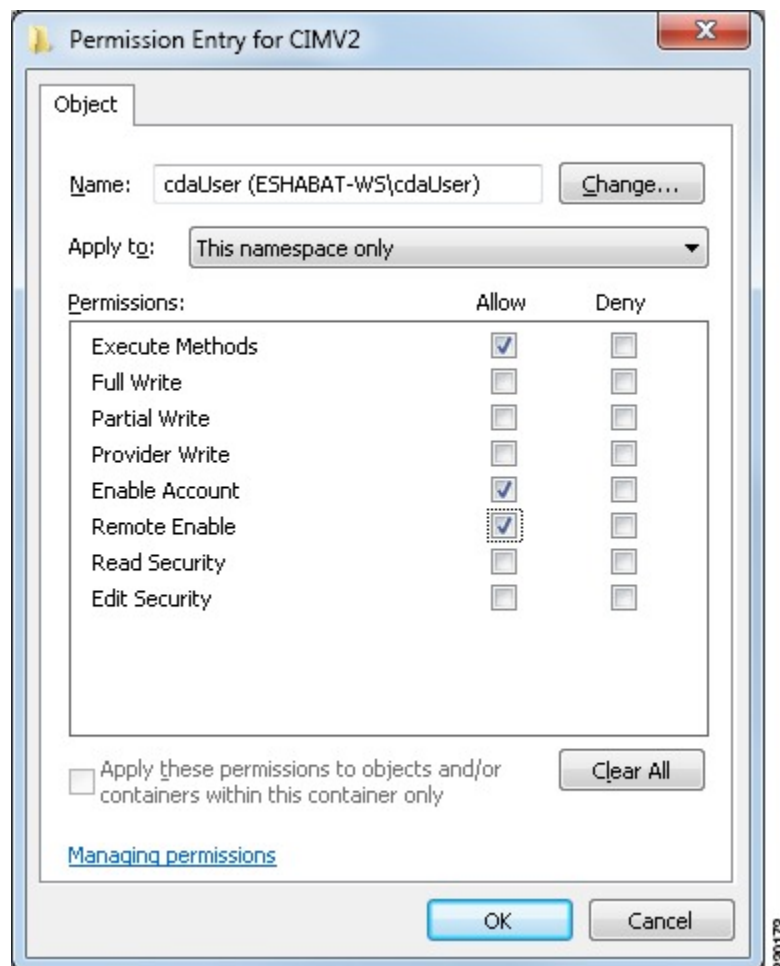


Set Permissions for Access to WMI Root/CIMv2 Name Space

By default, Active Directory users do not have permissions for the Execute Methods and Remote Enable. You can grant access using the wmicmgmt.msc MMC console.

- Step 1** Click Start > Run and type `wmicmgmt.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.

Figure 7: Required Permissions for WMI Root\CIMv2 Name Space



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 .

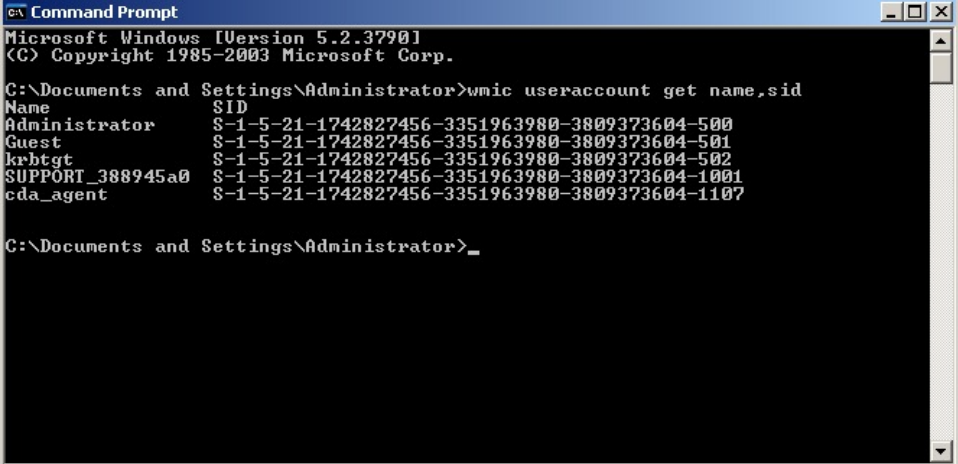
Step 2 Use the following command from the command line, also shown in the diagram below, to list all the SID accounts.

```
wmic useraccount get name,sid
```

You can also use the following command for a specific username and domain:

```
wmic useraccount where name="cdaUser" get domain,name,sid
```

Figure 8: List All the SID Accounts



```

c:\ Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>wmic useraccount get name,sid
Name SID
Administrator S-1-5-21-1742827456-3351963980-3809373604-500
Guest S-1-5-21-1742827456-3351963980-3809373604-501
krbtgt S-1-5-21-1742827456-3351963980-3809373604-502
SUPPORT_388945a0 S-1-5-21-1742827456-3351963980-3809373604-1001
cda_agent S-1-5-21-1742827456-3351963980-3809373604-1107

C:\Documents and Settings\Administrator>_
  
```

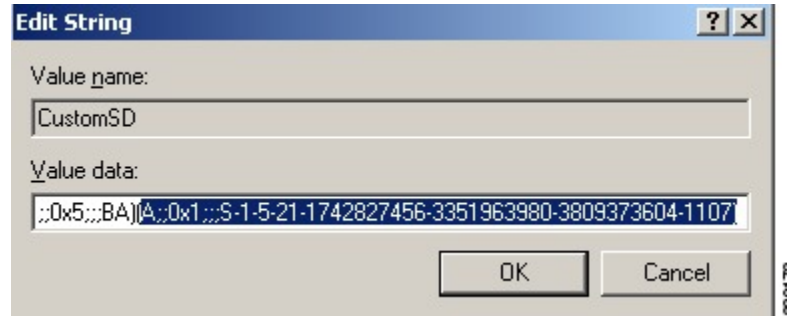
Step 3 Find the SID, open the Registry Editor, and browse to the following location:

```
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 cda_agent account (SID - S-1-5-21-1742827456-3351963980-3809373604-1107), enter (A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107).

Figure 9: Edit CustomSD String



- 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**.

Inline Posture Node

An Inline Posture node is a gatekeeping node that is positioned behind network access devices such as Wireless LAN Controllers (WLC) and VPN concentrators on the network. The Inline Posture node enforces access policies after a user has been authenticated and granted access, and handles change of authorization (CoA) requests that a WLC or VPN are unable to accommodate. Cisco ISE allows you to have two Inline Posture nodes that can take on primary or secondary roles for high availability.

The Inline Posture node must be a dedicated node. It must be dedicated solely for inline posture service, and cannot operate concurrently with other Cisco ISE services. Likewise, due to the specialized nature of its service, an Inline Posture node cannot assume any persona. For example, it cannot act as an Administration node that offers administration service, or a Policy Service node that offers network access, posture, profile, and guest services, or a Monitoring node that offers monitoring and troubleshooting services for a Cisco ISE network.

The Inline Posture persona is not supported on the Cisco ISE 3495 platform. Ensure that you install the Inline Posture persona on any one of the following supported platforms: Cisco ISE 3315, Cisco ISE 3355, Cisco ISE 3395, or Cisco ISE 3415.

You cannot access the web-based user interface of the Inline Posture nodes. You can configure them only from the PAN.

Inline Posture Node Installation

You must download the Inline Posture ISO (IPN ISO) image from Cisco.com and install it on any of the supported platforms. You must then configure certificates through the Command Line Interface (CLI). You can then register this node from the Admin portal.



Note

There is no separate Inline Posture ISO image for Release 1.31.4. Use the 1.2 IPN ISO image to install and set up an inline posture node.

After you install and set up the Inline Posture application, you must configure certificates before you can register the Inline Posture nodes. See the [Cisco Identity Services Engine Hardware Installation Guide](#) for more information.

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. The Inline Posture node cannot assume any other persona, due to its specialized nature. The Inline Posture node must be a dedicated node.

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 Administration Node (PAN). While defining your PAN, you must enable the Administration and Monitoring personas on that node. You can optionally enable the Policy Service persona on the PAN. After you complete the task of defining personas on the PAN, you can then register other secondary nodes to the PAN and define personas for the secondary nodes.

All Cisco ISE system and functionality-related configurations should be done only on the PAN. The configuration changes that you perform on the 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 PAN, you must enable the Monitoring persona. After you register a Monitoring node in your deployment, you can edit the 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. After the node status turns green, it takes about five minutes for the Cisco ISE application server to restart and run to complete the secondary ISE node configuration.

Cisco ISE Node Deregistration

To remove a node from a deployment, you must deregister it. When you deregister a secondary node from the 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.



Note

You cannot deregister a PAN.

Automatic Restart of the Cisco ISE Application Server

The application server in an Cisco ISE node restarts which causes a delay when you make any of the following changes:

- 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

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 or Inline Posture node. For Administration, Policy Service, and Monitoring capabilities, you must choose an ISE node. For Inline Posture service, you must choose the Inline Posture 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 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 Cisco ISE nodes, and restarting Cisco ISE nodes.
- (Optional) Deregister a secondary Cisco ISE node from the 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 PAN and the standalone node that you are about to register as a secondary node are running the same version of Cisco ISE.
- Ensure that the database passwords of the primary and secondary nodes are the same. If these passwords are set differently during node installation, you can modify them using the following commands:
 - **application reset-passwd ise internal-database-admin**
 - **application reset-passwd ise internal-database-user**

Menu Options Available on Primary and Secondary Nodes

Cisco ISE nodes provide you an Admin portal that you can use to perform your tasks. 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 Administration Node (PAN). For some tasks, you must use the secondary nodes. Therefore, the user interface of the secondary nodes provides limited menu options based on the personas 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 personas.

Table 3: Cisco ISE Nodes and Available Menu Options

Cisco ISE Node	Available Menu Options
All Nodes	<ul style="list-style-type: none"> • View and configure system time and NTP server settings. • Install server certificate, manage certificate signing request. <p>Note The server certificate operations must be performed directly on each individual node. 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.</p>
Primary Administration Node	All menus and submenus.
Active Monitoring Node	<ul style="list-style-type: none"> • Home and operations menus. • Provides redundant access to monitoring data that can be accessed from both the Primary and the Active Monitoring nodes.
Policy Service Nodes	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.
Secondary Administration Node	<p>Option to promote the secondary Administration node to become the PAN.</p> <p>Note After you have registered the secondary nodes to the PAN, while logging in to the Admin portal of any of the secondary nodes, you must use the login credentials of the PAN.</p>

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 reimaging 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**.
 - Step 2** Check the check box next to the Cisco ISE node that you want to configure, and click **Edit**.
 - Step 3** Enter the values as required and click **Save**.
-

Configure a Primary Administration Node

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

-
- Step 1** Choose **Administration > System > Deployment**.
The Register button will be disabled initially. To enable this button, you must configure a PAN.
 - Step 2** Check the check box next to the current node, and click **Edit**.
 - Step 3** Click **Make Primary** to configure your 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

After you register the secondary node, the configuration of the secondary node is added to the database of the primary node and the application server on the secondary node is restarted. After the restart is complete, the secondary node will be running the personas and services that you have enabled on it. You can view all the configuration changes that you make from the Deployment page of the PAN. However, expect a delay of 5 minutes for your changes to take effect and appear on the Deployment page.

Before You Begin

Ensure that the primary node's Certificate Trust List (CTL) has the appropriate certificate authority (CA) certificates to validate the HTTPS certificate of the secondary node that you are going to register. When you import the secondary node's certificate into the CTL, check the **Trust for authentication within ISE** check box for the PAN to validate the secondary node's certificate.

The certificates that you import into the CTL of the PAN are replicated to the secondary nodes.

Also, after you register the secondary node to the primary node, if you change the HTTPS certificate on the secondary node, you must import the appropriate CA certificates into the CTL of the primary node.

We recommend that you decide on the type of node (Cisco ISE or Inline Posture) at the time of registration. If you want to change the node type later, you have to deregister the node from the deployment, restart Cisco ISE on the standalone node, and then reregister it.

If you plan to deploy two Administration nodes for high availability, register the secondary Administration node before you register the other secondary nodes. If you register the nodes in this sequence, you do not have to restart the secondary ISE nodes after you promote the secondary Administration node as your primary.

If you plan to deploy multiple Policy Service nodes running Session services with mutual failover among these nodes, place the Policy Service nodes in a node group. You must create the node group before you register the nodes.

-
- Step 1** Log in to the PAN.
- Step 2** Choose **Administration > System > Deployment**.
- Step 3** Choose **Register > Register an Cisco ISE Node** to register a secondary Cisco ISE node.
- Step 4** Enter a DNS-resolvable hostname or IP address of the secondary Cisco ISE node.
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 PAN. Otherwise, node registration fails. You must have previously defined the IP address and the FQDN of the secondary node in the DNS server.
- Step 5** Enter a UI-based administrator credential for the standalone node in the Username and Password fields.
- Step 6** Click **Next**.
Cisco ISE contacts the secondary node, obtains some basic information such as the hostname, default gateway, and so on, and displays it.
If you have chosen to register a secondary Cisco ISE node, you can edit the configuration of the secondary node.
If you have chosen to register a secondary Inline Posture node, no additional configuration needs to be performed at this point.
- Step 7** Click **Save**.
-

After a secondary node is registered successfully, you will receive an alarm on your PAN that confirms a successful node registration. If the secondary node fails to register with the PAN, the alarm is not generated. When a node is registered, the application server on that node is restarted. After successful registration and database synchronization, enter the credentials of the primary administrative node to log in to the user interface of the secondary node.

**Note**

In addition to the existing Primary node in the deployment, when you successfully register a new node, no alarm corresponding to the newly registered node is displayed. The Configuration Changed alarms reflect information corresponding to the newly registered nodes. You can use this information to ascertain the successful registration of the new node.

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

Register an Inline Posture Node

We recommend that you decide on the type of node (Cisco ISE or Inline Posture) at the time of registration. If you want to change the node type later, you have to deregister the node from the deployment, restart Cisco ISE on the standalone node, and then reregister it.

Before You Begin

- Ensure that the primary node's Certificate Trust List (CTL) has the appropriate certificate authority (CA) certificates to validate the HTTPS certificate of the secondary node that you are going to register.
- After you register the secondary node to the primary node, if you change the HTTPS certificate on the secondary node, you must import the appropriate CA certificates into the CTL of the primary node.

-
- Step 1** Log in to the PAN.
- Step 2** Choose **Administration > System > Deployment**.
- Step 3** Click **Deployment** from the navigation pane on the left.
- Step 4** Choose **Register > Register an Inline Posture Node** to register a secondary Inline Posture node.
-

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 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 Administration Nodes with the 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 PAN.
 - Step 2** Choose **Administration** > **System** > **Deployment**.
 - Step 3** Check the check box next to the node that you want to synchronize with the PAN, and click **Syncup** to force a full database replication.
-

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-redirectioned sessions on the failed node.

**Note**

We recommend that you make all PSNs in the same local network part of the same node group. PSNs need not be part of a load-balanced cluster to join the same node group. However, each local PSN in a load-balanced cluster should typically be part of the same node group.

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 and TCP/7802.

-
- 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** 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 Cisco pxGrid Services

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

Before You Begin

- You need a Plus license to enable the Cisco pxGrid services.
- Cisco pxGrid services running on a Cisco ISE SNS 3415/3495 Appliance or in VMWare.
- When the Administrator node and the pxGrid node are the same, they are configured to use the same self signed certificate. In other deployments, the pxGrid node should be configured with a root certificate. Any client that connects to the pxGrid node should present the same root certificate or a certificate signed by the Administrator.
- If you are using a distributed deployment or upgrading from Cisco ISE 1.2, then you need to enable the pxGrid services in the certificates. To enable the pxGrid services, 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.
- If you have enabled FIPS mode in Cisco ISE 1.2, after upgrading to 1.4, pxGrid option will be disabled while you are generating or editing the certificates (including the self-signed and CA signed certificates).

Cisco pxGrid services do not run on FIPS-enabled Cisco ISE appliance, as the XCP server that is used to integrate Cisco pxGrid with Cisco ISE is not FIPS compliant. If FIPS mode was not enabled in Cisco ISE 1.2, after upgrading to 1.4, pxGrid option will be enabled for the certificates.

-
- 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.
-

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 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 PAN to confirm the persona or service change. If the persona or service change is not saved successfully, an alarm is not generated.
-

Manually Promote Secondary Administration Node To Primary

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

Before You Begin

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

-
- Step 1** Log in to the user interface of the Secondary Administration Node.
 - Step 2** Choose **Administration > System > Deployment**.
 - Step 3** In the Edit Node page, click **Promote to Primary**.
You can only promote a Secondary Administration Node to become the PAN. Cisco ISE nodes that assume only the Policy Service or Monitoring persona, or both, cannot be promoted to become the PAN.
 - Step 4** Click **Save**.
-

What to Do Next

If the node that was originally the PAN comes back up, it will be demoted automatically and become the Secondary Administration Node. 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.

Configure Primary Administration Node for Automatic Failover

Before You Begin

To enable the auto-failover feature, make sure that at least two nodes in your distributed setup assume the Administration persona and one node assume the non-Administration persona.

-
- Step 1** Log in to the user interface of the 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 PAN.
You can only promote a Secondary Administration Node to become the 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 PAN.
 - Step 4** Select the health check node for 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 PAN.
 - Step 5** Select the health check node for Secondary Administration Node, 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 Administration Node.
 - 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 Administration Node to the PAN, do the following:

- Manually sync the old 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.

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.



Caution 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 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.

You can view these changes from the Deployment page of the 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 PAN to confirm that the secondary node is deregistered successfully. If the secondary node fails to deregister from the 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 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 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 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 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 administration nodes and install it on the PAN.
 - Step 3** Restore the backup on the replaced PAN.
The restore script will try to sync the data on the Secondary Administration Node, but the secondary administration node is now a standalone node and the sync will fail. Data is set to the time the backup was taken on the PAN.
 - Step 4** Register the new node as a secondary server with the PAN.
-



Set Up Inline Posture

- [Role of Inline Posture Node in a Cisco ISE Deployment](#), page 71
- [Best Practices for Inline Posture Deployment](#), page 78
- [Inline Posture Node Guidelines](#), page 79
- [Inline Posture Node Authorization](#), page 82
- [Deploy an Inline Posture Node](#), page 84
- [Configure a High-Availability Pair](#), page 89
- [Configure Inline Posture Node as RADIUS Client in Administration Node](#), page 91
- [Remove an Inline Posture Node from Deployment](#), page 92
- [Health of an Inline Posture Node](#), page 92
- [Remote Access VPN Use Case](#), page 92
- [Collection of Inline Posture Node Logs](#), page 94
- [Kclick process in Inline Posture Node](#), page 95

Role of Inline Posture Node in a Cisco ISE Deployment

An Inline Posture node is a gatekeeper that enforces access policies and handles change of authorization (CoA) requests. An Inline Posture node is positioned behind the network access devices on your network that are unable to accommodate CoA requests, such as wireless LAN controllers (WLCs) and VPN devices.

After the initial authentication of a client using the EAP/802.1x and RADIUS protocols, the client must go through posture assessment. The posture assessment process determines whether the client should be restricted, denied, or allowed full access to the network. When a client accesses the network through a WLC or VPN device, an Inline Posture node is responsible for the policy enforcement and CoA that these devices are unable to accommodate.

**Note**

Starting from Release 1.3, Cisco ISE does not include a separate ISO image for Inline Posture. You can continue to use the existing Release 1.2 Inline Posture nodes in the deployment.

Inline Posture Policy Enforcement

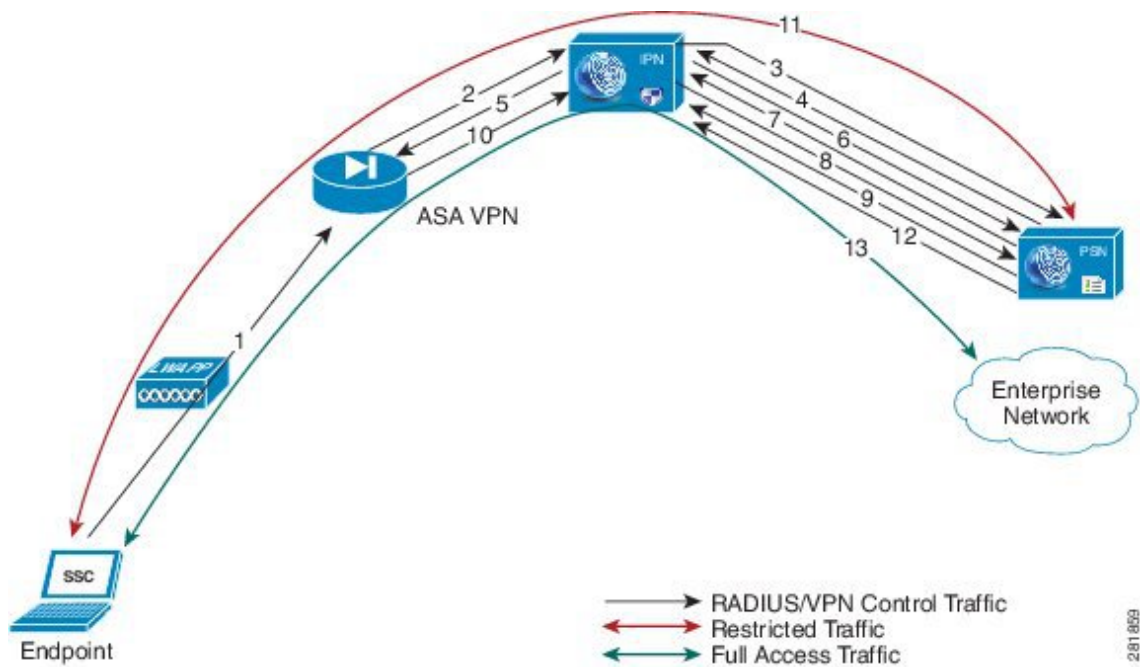
Inline Posture uses RADIUS proxy and URL redirect capabilities in the control plane to manage data plane traffic for endpoints. As a RADIUS proxy, Inline Posture is able to tap into RADIUS sessions between network access devices (NADs) and RADIUS servers. NADs can open full gate to client traffic. However, Inline Posture opens only enough to allow limited traffic from clients. The restricted bandwidth allows clients the ability to have an agent provisioned, posture assessed, and remediation completed. This restriction is accomplished by downloading and installing Downloadable Access Control Lists (DACLS) that are tailored for specific client flows.

When the client is compliant, a CoA is sent to the Inline Posture node by the Policy Service node, and full gate is opened by the Inline Posture node for the compliant client endpoint. The RADIUS proxy downloads the full-access DACL, installs it, and associates the client IP address to it. The installed DACL can be common for a number of user groups, and therefore duplicate downloads are not necessary as long as the DACL content does not change in the Cisco ISE servers.

Inline Posture Policy Enforcement Flow

The following figure illustrates the Inline Posture policy enforcement process and shows the flow for WLC enforcement for traffic to the Policy Service node. The access steps are similar for an inline deployment with VPN gateways.

Figure 10: Inline Posture Policy Enforcement Flow



- 1 The endpoint initiates a .1X connection to the wireless network.
- 2 The WLC, which is a NAD, sends a RADIUS Access-Request message to the RADIUS server, which is usually the Policy Service node (in this illustration, the RADIUS Access-Request message is sent to the Inline Posture node).

3 The Inline Posture node, acting as a RADIUS proxy, relays the Access-Request message to the RADIUS server.

4 After authenticating the user, the RADIUS server sends a RADIUS Access-Accept message back to the Inline Posture node.

There can be a number of RADIUS transactions between the Endpoint, WLC, Inline Posture node, and the Cisco ISE RADIUS server before the Access-Accept message is sent. The process described in this example has been simplified for the sake of brevity.

5 The Inline Posture node passes the Access-Accept message to the WLC, which in turn authorizes the endpoint access, in accordance with the profile that accompanied the message.

6 The proxied Access-Accept message triggers the Inline Posture node to send an Authorization-Only request to the Policy Service node to retrieve the profile for the session.

7 The Policy Service node returns an Access-Accept message, along with the necessary Inline Posture node profile.

8 If the access control list (ACL) that is defined in the profile is not already available on the Inline Posture node, the Inline Posture node downloads it from the Policy Service node using a RADIUS request (to the Cisco ISE RADIUS server).

9 The Cisco ISE RADIUS server sends the complete ACL in response. It is then installed in the Inline Posture data plane so that endpoint traffic passes through it.

There may be a number of transactions before the complete ACL is downloaded, especially if the ACL is too large for one transaction.

10 As the endpoint traffic arrives at the WLC, the WLC sends out a RADIUS Accounting-Start message for the session to the Inline Posture node.

The actual data traffic from the endpoint may arrive at the Inline Posture node untrusted side before the Accounting-Start message is received by the Inline Posture node. Upon receiving the RADIUS Accounting-Start message, the Inline Posture node learns the IP address of the endpoint involved in the session and associates the endpoint with the ACL, which is downloaded and installed earlier in the session. The initial profile for this client endpoint could be restrictive, to posture the client before being given full access.

11 Assuming the restrictive ACL allows access only to Cisco ISE servers, the endpoint is only allowed actions such as agent downloading and posture assessment over the data plane.

12 If the client endpoint is posture compliant (as part of the restricted communication with Cisco ISE services earlier), the Policy Service node initiates a RADIUS (CoA) with the new profile. Therefore, a new ACL is applied at the Inline Posture node for the session. The new ACL is installed immediately and applied to the endpoint traffic.

13 The endpoint is then capable of full access to the enterprise network, as a result of the new profile that was applied to the Inline Posture node.

A RADIUS stop message for a given session that is issued from the WLC resets the corresponding endpoint access at the Inline Posture node.

In a deployment, such as outlined in the example, when more endpoints connect to the wireless network, they are likely to fall into one of the identity groups that already have authenticated and authorized users connected to the network.

For example, there may be an employee, executive, and guest user that have been granted access through the outlined steps. This situation means that the respective restrictive or full-access profiles for those ID groups

have already been installed on the Inline Posture node. The subsequent endpoint authentication and authorization uses the existing installed profiles on the Inline Posture node, unless the original profiles have been modified during the Cisco ISE policy configuration. In the latter case, the modified profile with ACL is downloaded and installed on the Inline Posture node, replacing the previous version.

Trusted and Untrusted Interfaces

The following terminology plays a significant role in Inline Posture deployment:

- **Trusted**—The interface that talks to the Policy Service node and other trusted devices *inside* the Cisco ISE network. The trusted interface is always designated to Eth0 interface.
- **Untrusted**—The interface that talks to the WLC, VPN, and other devices *outside* the Cisco ISE network. The untrusted interface is always designated to Eth1 interface.

Dedicated Nodes Required for Inline Posture

Unlike other personas, Inline Posture is unable to share a node with other services. This inability to share a node means that Inline Posture must be a dedicated node that is registered to the PAN on your network.

Cisco ISE allows you to have up to two Inline Posture nodes configured as an active-standby pair for high availability.

Standalone Inline Posture Node in a Cisco ISE Deployment

A standalone Inline Posture node is simply a single Inline Posture node that provides services and works independently of all other nodes. You might choose to deploy a single standalone Inline Posture node for a network that serves a small facility, where redundancy is not a major concern.

Inline Posture High Availability

An Inline Posture high-availability deployment consists of two Inline Posture nodes that are configured as an active-standby pair. The active node acts as the RADIUS proxy and forwards all network packets until it fails and then the standby node takes over. As long as the active node is functioning properly, the standby node remains passive. However, should the active node falter, the standby node takes over to perform Inline Posture functionality.

The terms primary and secondary have different meanings with regard to Inline Posture high availability than they do in relation to Cisco ISE nodes. For Inline Posture high availability, primary and secondary denote the device that takes over the active state and the device that takes the standby role in case there is a contention, such as when both nodes boot up at the same time. The terms active and standby are representative of high-availability states. A primary or secondary Inline Posture node can be in either an active or standby state. The secondary Inline Posture node is read-only, and cannot be used for configuration of any kind, even high availability.

When you configure an Inline Posture high-availability pair, the primary node has more options available for editing. That is because you make all configuration changes on the primary node. Configuration changes made to the primary node are automatically populated onto the secondary node. For this reason, the secondary node is read-only.

An Inline Posture high-availability pair consists of two physical Inline Posture nodes configured as a cluster that have heartbeat links on the eth2 and eth3 interfaces, and are connected by dedicated cables.

The eth2 and eth3 interfaces of both nodes communicate with heartbeat protocol exchanges to determine the health of the nodes. Each Inline Posture node has its own physical IP addresses on the trusted and untrusted Ethernet interfaces, but a separate service IP address must be assigned to the cluster as a whole.



Note The service IP address, also called a virtual IP address, is required for RADIUS authentication purposes. You assign the service IP address to both the trusted and untrusted interfaces for both nodes of the active-standby pair, thus making the service IP address the address of the cluster, representing it as a single entity to the rest of the network.

Automatic Failover in Inline Posture Nodes

Inline Posture stateless high-availability deployment has an active-standby pair node configuration, where the standby node acts as a backup unit and does not forward any packets between the interfaces. Stateless means that sessions that have been authenticated and authorized by an active node are automatically authorized again after a failover occurs.

The standby node monitors the active node using the heartbeat protocol (using eth2 and eth3 interfaces), which requires that messages are sent at regular intervals between the two nodes. If the heartbeat stops or does not receive a response back in the allotted time, failover occurs and recovery action takes place.

A heartbeat is a message that is sent from one node in an Inline Posture high-availability pair to the other member of the pair at regular intervals. If a heartbeat is not received for an extended period of time, usually several heartbeat intervals, the node that should have sent the heartbeat is assumed to have failed. If it is the primary Inline Posture node that fails, the secondary node takes over so there is no disruption in service.

If the heartbeats simultaneously go down for both Inline Posture high-availability nodes, a partitioning state may ensue. A partitioning state is a condition where both nodes assume that the other has totally failed, and both try to take over active control.

In addition to the heartbeat monitor, an optional (but highly recommended) link-detect mechanism is available. With the use of this mechanism, Inline Posture trusted and untrusted interfaces ping an external IP address from their respective interfaces. If both nodes are unable to ping the external IP address, then failover does not occur. However, if either of the nodes becomes unreachable, the node that is functional automatically becomes the active node.

When failover occurs:

- 1 The standby Inline Posture node takes over the service IP address.
- 2 The administrator corrects the failed node and reverts to an earlier configuration, as needed.

When a failed node is brought back online, a manual sync operation to update the node with the most current information is required.

- 3 Active sessions are automatically reauthenticated and authorized.

Inline Posture Operating Modes

The Inline Posture operating mode that you choose depends largely on the architecture of your existing network. Cisco ISE supports the following operating modes:

Inline Posture Routed Mode

The Inline Posture routed mode acts as a Layer 3 “hop” in the wire, selectively forwarding packets to specified addresses. This mode provides the ability to segregate network traffic, allowing you to specify users who have access to selected destination addresses.

In routed mode, the Inline Posture node operates as a Layer 3 router, and becomes the default gateway for the untrusted network with its managed clients. All traffic between the untrusted and trusted networks passes through the Inline Posture node, which applies the IP filtering rules, access policies, and other traffic-handling mechanisms that you decide to configure.

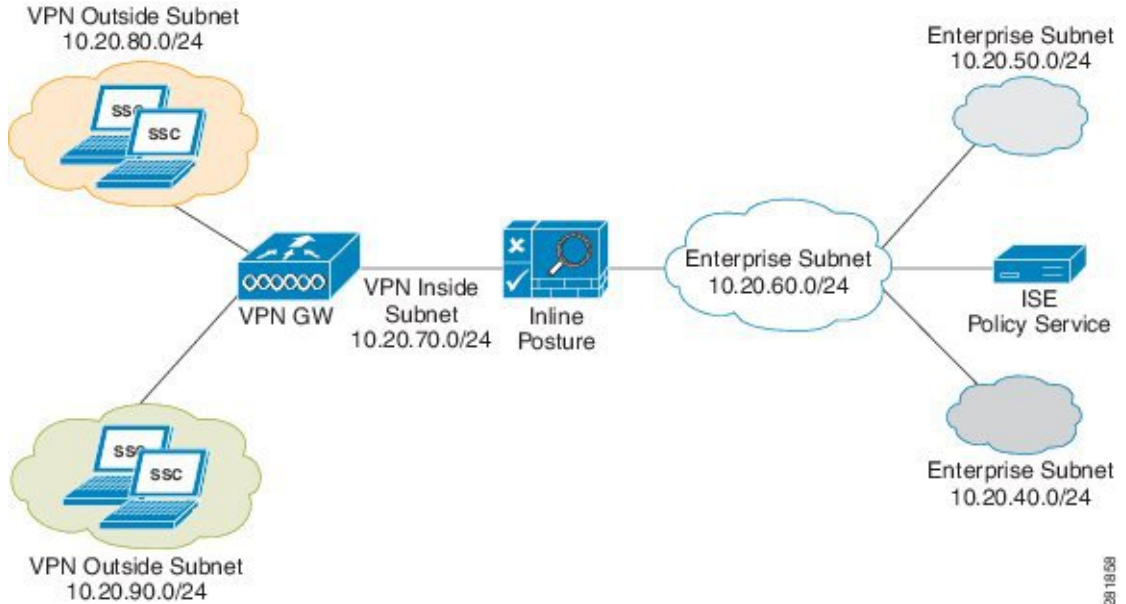
When you configure Inline Posture in routed mode, you must specify the IP addresses of its two interfaces:

- Trusted (Eth0)
- Untrusted (Eth1)

The trusted and untrusted addresses should be on different subnets. Inline Posture can manage one or more subnets, with the untrusted interface acting as a gateway for the managed subnets.

The following figure illustrates an Inline Posture routed mode configuration. In this example, Inline Posture is a hop for the client traffic from the VPN gateway (GW) en route to the Policy Service node. Inline Posture requires that static routes be configured for subnets 10.20.80.0/24 and 10.20.90.0/24 toward the VPN gateway, just like any other router. The enterprise router on the trusted side of the network also requires that the static routes are configured for the same subnets toward the Inline Posture node.

Figure 11: Inline Posture Routed Mode Configuration



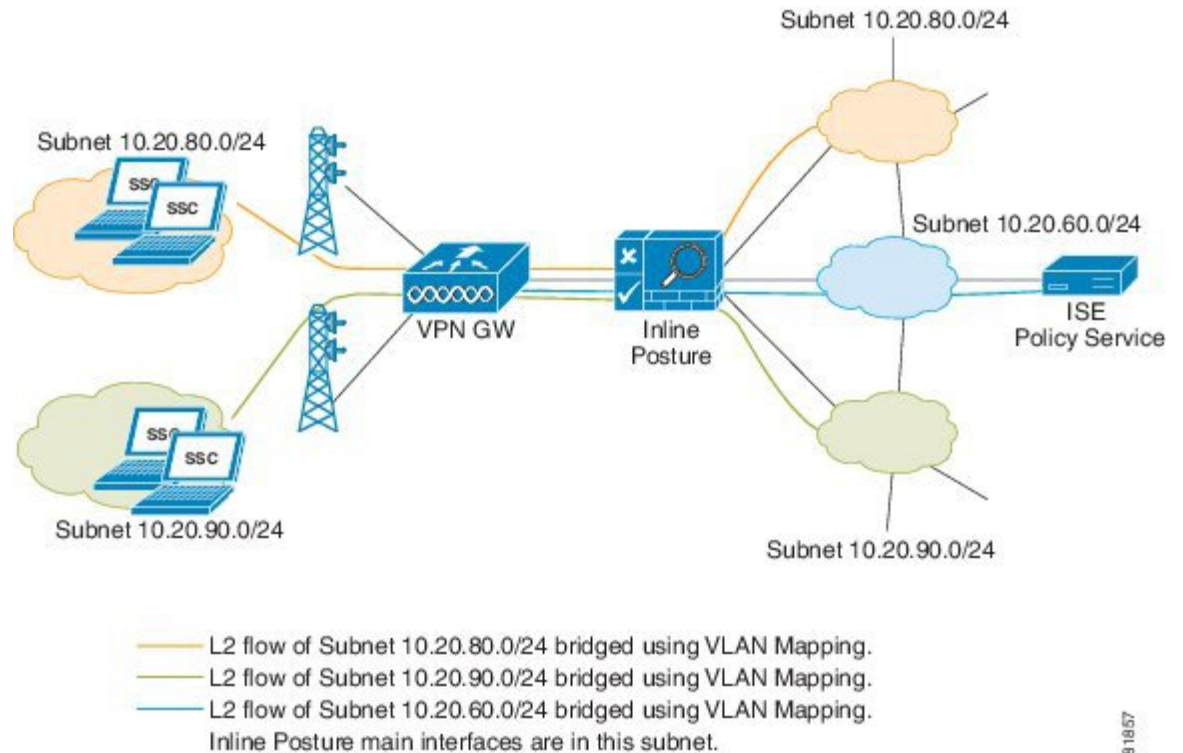
Inline Posture Bridged Mode

The Inline Posture bridged mode acts as a Layer 2 “bump” in the wire, forwarding packets without regard to the destination address.

In bridged mode, the Inline Posture node operates as a standard Ethernet bridge. This configuration is typically used when the untrusted network already has a gateway, and you do not want to change the existing configuration.

The following figure shows the Inline Posture node acting as a bridge for the Layer 2 client traffic from the WLC to the Cisco ISE network, managed by the Policy Service node. In this configuration, Inline Posture requires subnet entries for the 10.20.80.0/24 and 10.20.90.0/24 subnets to be able to respond to and send Address Resolution Protocol (ARP) broadcasts to the correct VLANs.

Figure 12: Inline Posture Bridged Mode Configuration



When the Inline Posture node is in bridged mode, the following conditions apply:

- Inline Posture eth0 and eth1 interfaces can have the same IP address.
- All end devices in the bridged subnet must be on the untrusted network.

Inline Posture Maintenance Mode

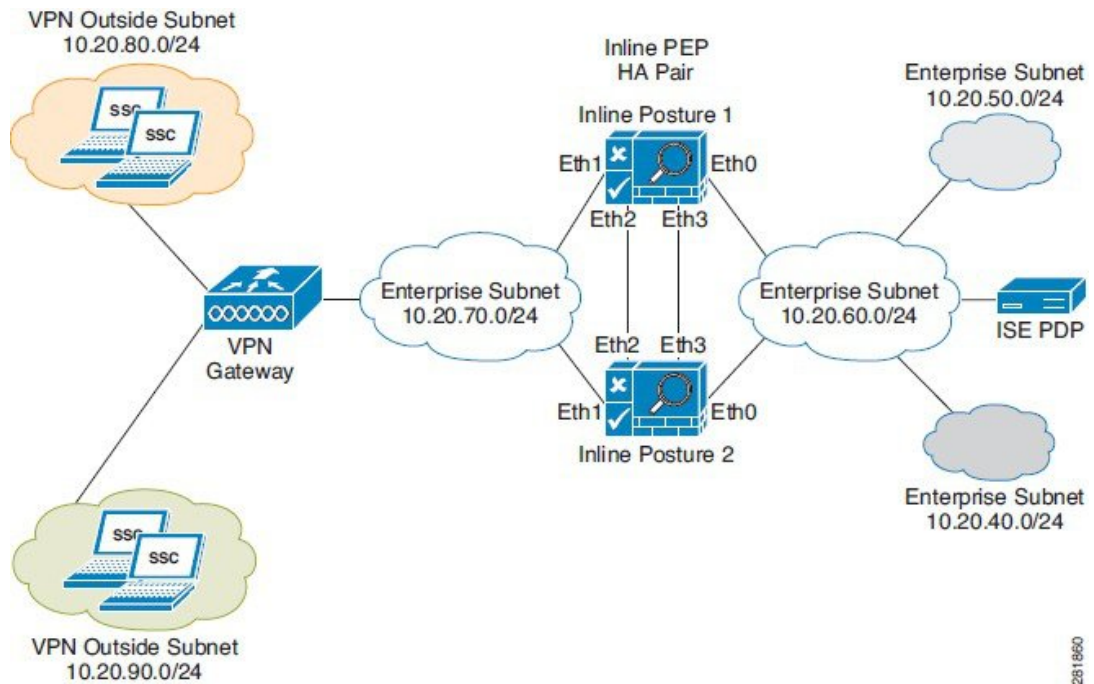
The Inline Posture maintenance mode takes the node offline so that you can perform administrative procedures. This mode is also the default mode of a node when it first comes onto the network, and before you perform other configurations.

Inline Posture High Availability in Routed and Bridged Modes

The following figure shows an example of an Inline Posture high-availability routed mode configuration. Note the dedicated cables that connect the eth2 and eth3 interfaces between the two nodes to facilitate the heartbeat communication that checks for failure in the active node.

In this example, the untrusted IP address for Inline Posture 1 can be 10.20.70.101, and the untrusted IP address for Inline Posture 2 can be 10.20.70.102. However, the service IP address for both nodes on the untrusted side of the network would be 10.20.70.100. The active Inline Posture node in the pair, at any point of time, assumes the service IP address on the untrusted side of the network. The same holds true for the trusted side of the network.

Figure 13: Inline Posture High-Availability Routed Mode Configuration



In a bridged mode, Inline Posture eth0 and eth1 interfaces should have IP addresses in the same subnet. Having the same IP address is recommended. Any devices on the trusted side of the network that have IP addresses in the subnets that are managed by an Inline Posture in bridged mode, must have an explicit static route configured at the Inline Posture node. This configuration is necessary because by default, Inline Posture assumes that the subnet that it manages (as configured on the Managed Subnets user interface page) lies entirely on the untrusted side of the network.

Best Practices for Inline Posture Deployment

You can follow the best practices listed here to manage your Inline Posture deployment efficiently.

Use Filters to Define Access Privileges

Consider the following when configuring filters for Inline Posture:

- In a typical implementation, Inline Posture enforces authentication requirements on endpoints that attempt to access the network. Device and subnet filters are used to validate or deny WLC and VPN devices.
- For certain devices, you may want to bypass authentication, posture assessment, role assignment, or any combination thereof. Common examples of bypassed device types include printers, IP phones, servers, nonclient machines, and network devices.

Inline Posture matches the MAC, MAC and IP, or subnet address to determine whether the bypass function is enabled for a device. You can choose to bypass policy enforcement or to forcibly block access.



Caution

Do not configure the MAC address in a MAC filter for a directly connected ASA VPN device without also entering the IP address. Without the addition of the optional IP address, VPN clients are allowed to bypass policy enforcement. This bypass happens because the VPN is a Layer 3 hop for clients, and the device uses its own MAC address as the source address to send packets along the network toward the Inline Posture node.

Configure Managed Subnets and Static Routes

Consider the following when configuring managed subnets for Inline Posture:

- Configure a managed subnet for Inline Posture. A managed subnet configuration ensures that the Inline Posture node can send Address Resolution Protocol (ARP) queries with the appropriate VLAN IDs for the client devices on the untrusted interface. Configure the untrusted (authentication) VLAN in the VLAN ID field for the managed subnet.
- Configure managed subnets for endpoints in Layer 2 proximity of the Inline Posture node, such as, a WLC that delivers packets directly to the untrusted interface of the Inline Posture node.
- Configure an IP address and not a subnet address. This configuration ensures that the ARP requests that Inline Posture sends have a valid source IP address.
- Ensure that subnets on the trusted side of the Inline Posture node are different from the subnets on the untrusted side.
- Ensure that an Administration node, Policy Service node, and Monitoring node are not on the same subnet as the Inline Posture node, unless you have defined a static route.

Consider the following when configuring static routes for Inline Posture:

- Configure static routes for endpoints that are more than one hop away (Layer 3) from the Inline Posture node.
- Configure static routes for all downstream host networks that are typical of VPN address pools.

Configure High-Availability Pair

Consider the following when configuring Inline Posture for high availability:

- Assign a service IP address (also known as a virtual IP) for each side of the Inline Posture interfaces, trusted (eth0) and untrusted (eth1).
- Specify link-detect IP addresses for the trusted (eth0) and untrusted (eth1) interfaces. Link-detect appears as an optional setting in the user interface, but is highly recommended.

Inline Posture Node Guidelines

Before you configure an Inline Posture node in a distributed deployment, read and understand the following statements:

- 1 The Inline Posture node is supported only on Cisco ISE-3300 series and SNS-3415 appliances. It is not currently supported on Cisco SNS-3495 appliance or as a virtual appliance.
- 2 Inline Posture is unable to run concurrently with Administration, Policy Service, or Monitoring personas and, therefore, is a dedicated node.
- 3 An Inline Posture node must be registered to the PAN on your network.
- 4 For each deployment instance of an Inline Posture node, you can deploy a standalone node, or an active-standby pair.
- 5 At any network entry point, like VPN headend using ASA or group of ASAs in an HA cluster, a maximum of 2 Inline Posture nodes can be deployed as active-standby pair for high-availability. You can have several HA pairs in a deployment.
- 6 Inline Posture nodes are similar to network access devices (NAD) in function from the perspective of Cisco ISE node. Inline Posture nodes can serve as multiple NADs like switches, Wireless Lan Controllers, and VPN devices. Based on the deployment needs, you can deploy multiple instances of Inline Posture nodes. To determine the maximum number of deployment instances, treat the Inline Posture nodes as access devices.
- 7 For an Inline Posture high-availability, two nodes are configured as an active-standby pair. One node is designated as the primary node and the other as the secondary node. The primary node becomes the active node when both nodes come up at the same time.
- 8 For an Inline Posture active-standby pair configuration, all configuration must be applied from the ISE administrative user interface. The standby node configuration displays only basic tables when viewed from the ISE administrative user interface.
- 9 You can synchronize an Inline Posture active node configuration to its peer standby node from the Failover tab of the active node. For more information, see [Synchronize an Inline Posture Node](#), on page 90.



Note

If you have a WLC authentication, authorization, and accounting (AAA) server (Cisco 2100 or 4400 Series Wireless LAN controllers) on your network, the RADIUS authentication server timeout value needs to be set to a minimum of 30 seconds. This minimum value ensures that RADIUS failover will work in conjunction with Inline Posture. See the WLC server hardware documentation for more information.

- 10 Registering an Inline Posture node results in system restart. High-availability changes and changes to infrastructure configurations such as the eth1 IP address or Inline Posture mode require a system restart. The restart is automatic. However, to manually restart the node from the CLI, use the **application stop ise** and **application start ise** commands.
- 11 After you register an Inline Posture node to the Administration node, you are not allowed to change the eth0 (Trusted) IP address through the Admin portal. The reason for this is that, if you change the eth0 IP address of a registered Inline Posture node, it cannot communicate with the Administration node. Any attempted communication between the Inline Posture node and Administration node then fails, leading to a potential exception.



Note

It is highly recommended that you not change the IP address of an Inline Posture node from the CLI after it has been registered on the Cisco ISE network.

**Caution**

The Inline Posture node's untrusted interface should be disconnected when the Inline Posture node is being configured. If the Inline Posture node's trusted and untrusted interfaces are connected to the same VLAN during initial configuration and the Inline Posture node initially starts after changing its persona, multicast packet traffic gets flooded out of the untrusted interface. This multicast storm can potentially bring down devices that are connected to the same subnet or VLAN. The Inline Posture node at this time is in Maintenance mode.

Inline Posture Node Authorization

The following images illustrate the client authorization flow and session recovery using Lazy Fetch mechanism for Inline Posture node.

Figure 14: Inline Posture Node Client Authorization Flow

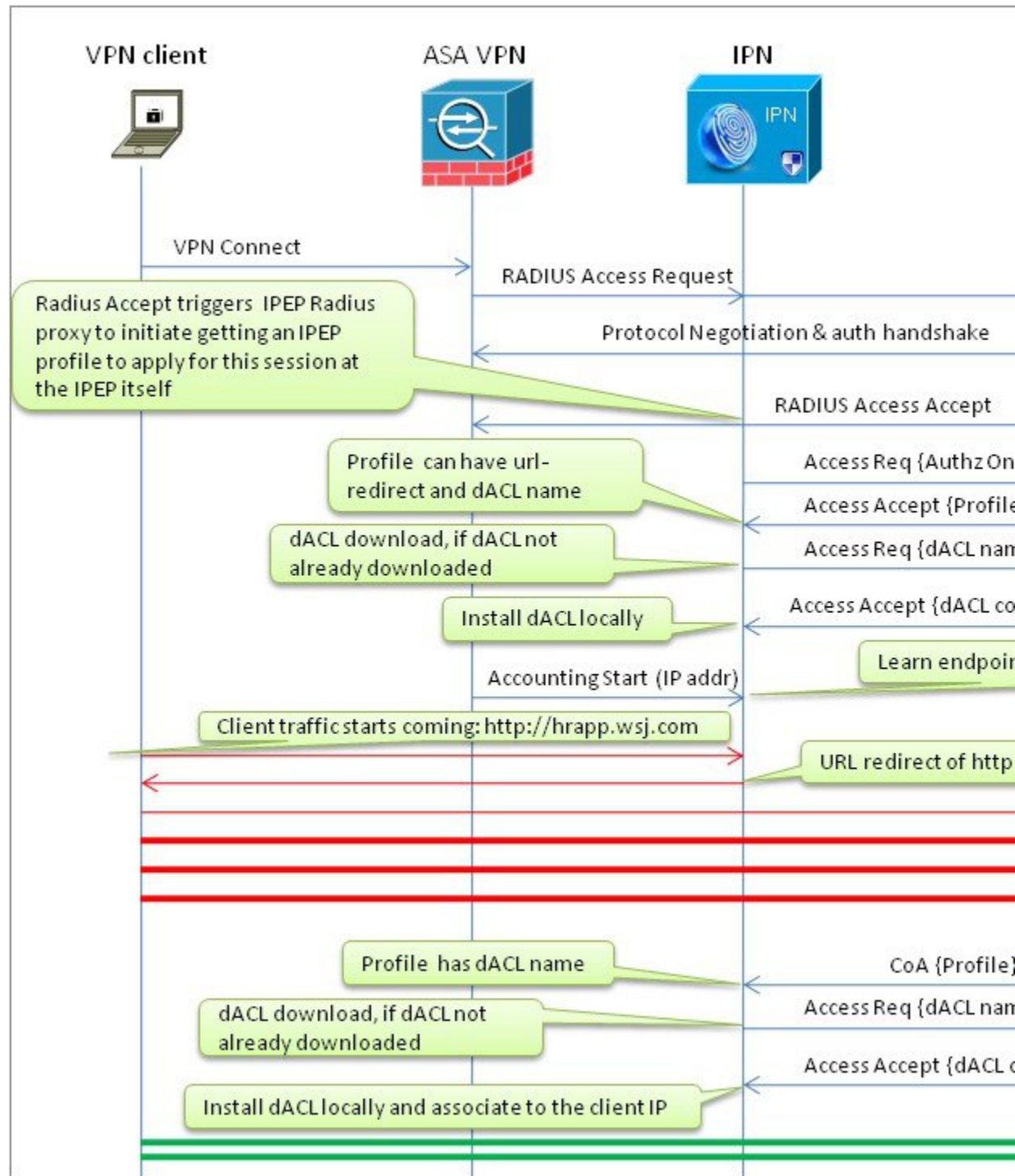
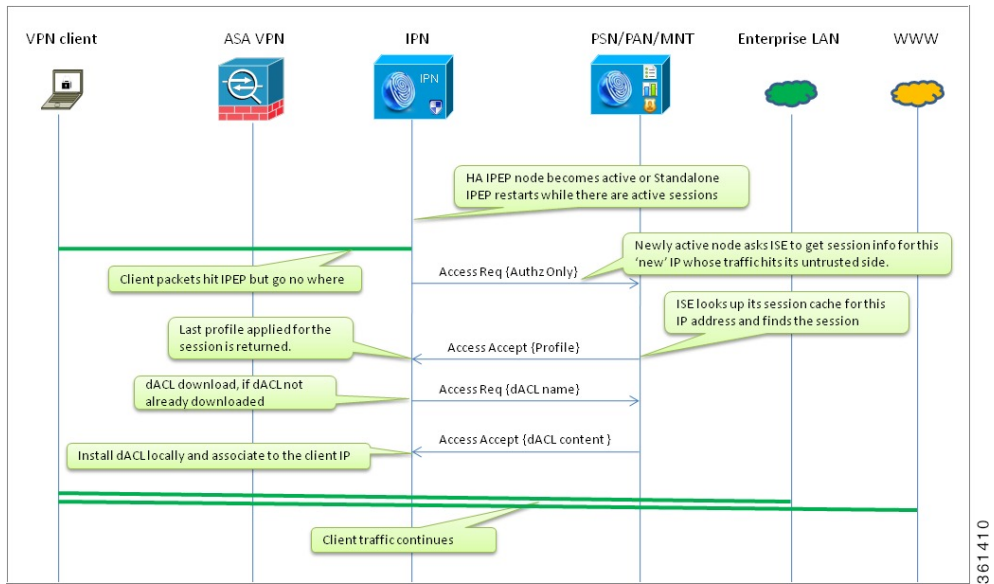


Figure 15: Inline Posture Node Session Recovery Using Lazy Fetch Mechanism



Inline Posture Node Session Removal due to Client Disconnect

When a wireless client is wandering off from the WLC control, the WLC is required to send a RADIUS Accounting Stop similar to the VPN gateway to ensure that the Inline Posture node cleans up the session corresponding to the client.

Deploy an Inline Posture Node

The initial process for deploying an Inline Posture node is the same, whether it is intended to be a standalone node or part of an active-standby pair.



Note Inline Posture is supported on the Cisco ISE 3415, ISE 3315, ISE 3355, and ISE 3395 platforms.

- Step 1** Configure an Inline Posture node.
- Step 2** Create Inline Posture Downloadable Access Control Lists.
- Step 3** Create Inline Posture node profiles.
- Step 4** Create an Inline Posture authorization policy.

Configure an Inline Posture Node

Inline Posture is a dedicated node registered to the Administration node. You configure Inline Posture from the administration console, and that configuration is then replicated to the Inline Posture node. A copy of the configuration is stored locally in the administration database. After an Inline Posture node is registered, it is rebooted.

To introduce an Inline Posture node in your Cisco ISE network, you must first register the Inline Posture node with the PAN, configure the Inline Posture settings, and then create authorization profiles and policies that establish the Inline Posture gatekeeping policies.

The Inline Posture node is a RADIUS proxy that interfaces with NADs as their RADIUS server, making the NADs (VPN gateway, WLC) RADIUS clients. As a proxy, Inline Posture interfaces with the Policy Service node as a client making the Policy Service node its RADIUS server.



Note After completing the following procedure, a NAD entry is automatically created for the Inline Posture node. For a standalone node, the IP address for that node is used. For a high-availability pair, the service IP address for the active node is used.

Before You Begin

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

Inline Posture is not supported on the Cisco ISE 3495 platform. Ensure that you install Inline Posture on any one of the following supported platforms: ISE 3315, ISE 3355, ISE 3395, or ISE 3415.

Follow and apply the guidelines for configuring certificates for Inline Posture. Refer to *Cisco Identity Services Engine Hardware Installation Guide, Release 1.2* for details.

Register the Inline Posture node with the PAN. All nodes must be registered with the PAN to function as a member of the Cisco ISE distributed system.

RADIUS configuration is mandatory. At least one client and one server configuration is necessary. You need the corresponding shared secret information for both sides to complete this procedure.

Have all necessary configuration information for your installation on hand. For example, you might need the trusted and untrusted IP addresses, service IP address, IP addresses for other Cisco ISE nodes, shared secret information for the RADIUS configuration, management VLAN ID, WLC, or VPN IP address, and so on. Check with your system architect for a complete list of the information you will need.



Caution Do not configure the MAC address in a MAC Filter for a directly connected ASA VPN device without also entering the IP address. Without the addition of the optional IP address, VPN clients are allowed to bypass policy enforcement. This access happens because the VPN is a Layer 3 hop for clients, and the device uses its own MAC address as the source address to send packets along the network toward the Inline Posture node.

-
- Step 1** Choose **Administration > System > Deployment**.
- Step 2** Check the **Inline Posture node** check box in the Deployment Nodes page and click **Edit**.
- Step 3** Check the **Inline PEP** check box on the General Settings tab. The Administration, Monitoring, and Policy Service check boxes are automatically unchecked.
The tabs change to General Settings, Basic Information, Deployment Modes, Filters, Radius Config, Managed Subnets, Static Routes, Logging, and Failover.
- Note** A newly registered Inline Posture node comes up with a default IP address of 192.168.1.100, a subnet mask of 255.255.255.0, and a default gateway of 192.168.1.1. Change these values to fit your deployment in Step 3.
- Step 4** Click the following tabs and enter the appropriate information for the fields in the tabs.

- Basic Information
- Deployment Modes—A newly registered Inline Posture node comes up in maintenance mode. For production purposes, you must choose the Routed or Bridged mode.
- Filters—Enter the subnet address and subnet mask for the client device, or the MAC address and IP address of the device on which to filter. You can use MAC and subnet filters to bypass Inline Posture enforcement to certain endpoints or devices on the untrusted side of the network. For example, if VPN or WLC management traffic is required to pass through Inline Posture, you would not want to subject those particular NADs to Cisco ISE policy enforcement. By providing the MAC address and IP address for these NADs on a filter, you can then access the user interface or configuration terminal by way of Inline Posture without restrictions.
- Radius Config—RADIUS configuration is mandatory. At least one client and one server configuration is necessary for Inline Posture.
- Managed Subnets—For subnets of endpoints that are in Layer 2 proximity to the Inline Posture node (such as a WLC), you must configure managed subnets. This configuration requires an unused IP address in the same subnet as the managed subnet, along with the VLAN (if any) of the subnet. You can have multiple managed subnet entries. You must enter the following values: IP Address, Subnet Mask, VLAN ID, and Description.
 - Static Routes—Enter the subnet address, subnet mask, and choose **Trusted** or **Untrusted** from the Interface Type drop-down list. Repeat this step as needed for your configuration.

When the subnets of the endpoints under Cisco ISE control are Layer 3 away from the Inline Posture node, a static route entry is needed. For example, if a VPN gateway device (that sends managed subnet traffic to the Inline Posture untrusted interface) is two hops away, its client subnet needs to have a static route defined for Inline Posture. The network on the trusted side should know to send traffic to the Inline Posture trusted interface.
 - Logging—Click the **Logging** tab and enter the IP address and port number for the logging server, which is typically the Monitoring node.

An IP address and port (default 20514) for logging Inline Posture events are mandatory. This requirement ensures that the viable status of the Inline Posture node is displayed in the Cisco ISE dashboard in the System Summary dashlet, and that other log information regarding the nodes is available.
 - Failover—This tab is for Inline Posture High Availability configuration.

Step 5 Click **Save** . The Inline Posture node restarts automatically.

Step 6 To verify the automatically generated Inline Posture NAD listing, go to **Administration > Network Resources > Default Device**.
For a standalone node, the IP address for that node is used. For a high-availability pair, the service IP address for the active node is used.

What to Do Next

To complete the deployment of the Inline Posture node, you must create ACLs, authorization profiles, and authorization policy rules: unknown, compliant, and noncompliant.

**Note**

It is important to associate the appropriate downloadable access control list (DACL) with the corresponding profile. For example, the unknown DACL should be associated with the unknown authorization profile.

Create Inline Posture Downloadable Access Control Lists

Downloadable access control lists (DACLs) are building blocks for authorization profiles, and they provide the rules for the profiles to follow. Access control lists (ACLs) prevent unwanted traffic from entering the network by filtering source and destination IP addresses, transport protocols, and other variables, using the RADIUS protocol.

After you create DACLs as named permission objects, add them to authorization profiles, which you then specify as the result of an authorization policy.

Before You Begin

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

Step 1 Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.

Step 2 Click **Add**.

Step 3 Enter the name of the DACL and its description.

Step 4 Create the following DACLs:

- ipn-compliant (Permit All): Use the following syntax: permit ip any any
- ipn-noncompliant (Deny All): Use the following syntax: deny ip any any
- ipn-unknown (Pre-Posture): Use at least one ACL to allow supplicants and the Policy Service node to have access to each other for posture evaluation. This DACL can be used to block or quarantine users until they pass authentication. Here is an example syntax:


```
deny tcp any any eq 80
deny tcp any any eq 443
permit ip any 10.1.2.4 0.0.0.0
permit udp any any eq 53
deny ip any any
```

Step 5 Save the DACLs.

What to Do Next

Create Inline Posture node profiles.

Create Inline Posture Node Profiles

You must create three Inline Posture authorization profiles, as well as an authorization profile for a NAD.

All Inline Posture inbound profiles are automatically set to `cisco-av-pair=ipep-Authz=true` so that the Inline Posture node applies these rules instead of proxying them on to the NADs. The URL redirect is essential for client provisioning, as well as agent discovery redirection.

Before You Begin

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

-
- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Inline Posture Node Profiles**.
- Step 2** Click **Add**.
- Step 3** Enter a name and description for the authorization profile. Supported characters for the name field are: space, ! # \$ % & ' () * + , - . / ; = ? @ _ { .
- Note** You can configure a RADIUS Reply Message = NAD Profile, to see NAD Profile in the RADIUS log messages for Inline Posture. This configuration can be helpful for troubleshooting at a later time.
- Step 4** Create the following authorization profiles for Inline Posture that correspond to the DACLs you created. Specify the appropriate DACL for each of the following authorization profiles:
- IPN-Unknown-Compliant (Pre-Posture): This profile requires that you enter a URL redirect. To do this, check the URL Redirect check box.
The URL redirect appears in the Attributes Details field.
You are redirected to a web page where you download and install an agent. The agent then scans your system. If your system passes, you are automatically granted full access. If your system does not pass, you are denied access.
 - IPN-Compliant (Permit All)
 - IPN-Noncompliant (Deny All).
- Step 5** Click **Submit**.
-

What to Do Next

Create an Inline Posture authorization policy.

Create an Inline Posture Authorization Policy

Authorization policies provide the means for controlling access to the network and its resources. Cisco ISE lets you define a number of rules when creating authorization policies.

The elements that define the authorization policy are referenced when you create policy rules. Your choice of conditions and attributes defines the authorization profile.

Before You Begin

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

-
- Step 1** Choose **Policy > Authorization**.
- Step 2** Leave the default rules as is.
- Step 3** Create the following Unknown Posture Status Rule:
- Identity Group: Any
 - Condition: Session:PostureStatus EQUALS = Unknown
 - Permissions: IPN-Unknown-Compliant + nad-authorization-profile
- Step 4** Create the following Compliant Posture Rule:
- Identity Group: Any
 - Condition: Session:PostureStatus EQUALS = Compliant
 - Permissions: IPN-Compliant + nad-authorization-profile
- Step 5** Create the following Noncompliant Posture Rule:
- Identity Group: Any
 - Condition: Session:PostureStatus EQUALS = Noncompliant
 - Permissions: IPN-Noncompliant + nad-authorization-profile
- Step 6** Save the policy. The Inline Posture node deployment is now complete.
-

What to Do Next

Configure Inline Posture node as RADIUS client in Administration node.

Configure a High-Availability Pair

When you configure two Inline Posture nodes for high availability, you specify one node as the primary unit in the pair and it becomes the active node by default. The other becomes the secondary node, which is a standby unit in case of default.

A high-availability node failover prompts the standby node to take over the service IP address. After this process occurs, an administrator must correct the failed Inline Posture node and revert it to the earlier configuration as needed. Because high-availability failover is stateless, all active sessions are automatically reauthorized after a failover occurs.

In the example that is presented, the service IP address used for the bridged mode high availability pair is different from the physical IP addresses of the Inline Posture nodes, effectively creating a cluster. The WLC interacts with the cluster as a single unit, using the service IP address. For this reason, the service IP is defined for the trusted and untrusted networks.

**Note**

Both nodes in a high availability pair must use the same mode, either bridged or router. Mixed modes are not supported on Inline Posture high availability pairs.

Before You Begin

- To perform the following task, you must be a Super Admin or System Admin.
- You should have successfully configured two (2) Inline Posture nodes, and registered them on the Cisco ISE network.
- The eth2 and eth3 interfaces of both nodes in an Inline Posture high availability pair (primary and secondary) communicate with heartbeat protocol exchanges to determine the health of the nodes. For the heartbeat to work, you must connect the eth2 interface of the primary Inline Posture node to the eth2 interface of the secondary node using an Ethernet cable. Likewise, the eth3 interface of the primary Inline Posture node must be connected to the eth3 interface of the secondary node with an Ethernet cable.
- For RADIUS purposes, you need a service IP address that you will assign to both the trusted and untrusted interfaces of the Inline Posture active-standby cluster during the course of this procedure.
- Have all necessary network configuration information for your installation on hand. Check with your system architect for a complete list of information you will need.

-
- Step 1** Choose **Administration > System > Deployment**.
- Step 2** Check the check box next to the Inline Posture node that you want to designate as the primary node, and click **Edit**.
- Step 3** On the General Settings tab, verify the node name, that the Inline PEP check box is selected, then choose **Active** as the HA Role from the drop-down list.
- Step 4** Click the **Failover** tab, and check the **HA Enabled** check box.
- Step 5** Enter the appropriate information in the fields.
- Step 6** Click **Save**. Both Inline Posture nodes restart. When the nodes come back up, they are configured as primary and secondary, according to the settings you specified.
- Step 7** Verify the node status by checking the check box next to it, and then clicking the **Failover** tab. Ensure that your primary and secondary Inline Posture nodes are configured correctly.
-

What to Do Next

Configure Inline Posture node as RADIUS Client in administration node.

Synchronize an Inline Posture Node

When a node in a high-availability pair is down and configuration changes are made to the single active node, there is no mechanism that automatically populates the failed node with the new configuration when it comes back up. The Sync-up Peer Node button that appears in the Inline Posture high-availability user interface on the active node, allows you to manually synchronize the standby node with the latest Inline Posture database from the active node.

Before You Begin

- You must be a Super Admin or System Admin.
- You must configure two Inline Posture nodes.
- You must establish a relationship between the two nodes.

-
- Step 1** Choose **Administration** > **System** > **Deployment**.
- Step 2** Check the check box next to the Inline Posture node that you want to sync with the other node (usually the active node), and click the **Edit** icon.
- Step 3** Click the **Failover** tab.
- Step 4** Click **Sync Peer Node**. Data from the selected node is automatically transferred to its peer node.
-

Configure Inline Posture Node as RADIUS Client in Administration Node

For an Inline Posture node to act as a RADIUS proxy, you must add it as a RADIUS client in the Administration node.

Before You Begin

- You must be a Super Admin or System Admin.
- You must deploy Inline Posture in your Cisco ISE deployment.

-
- Step 1** Choose **Administration** > **Network Resources** > **Network Devices**.
- Step 2** In the Network Devices navigation panel, click **Network Devices**.
- Step 3** Enter a Name and an optional Description for the device.
- Step 4** Enter the IP address of the Inline Posture node.
- For a standalone Inline Posture node, enter the IP address for the trusted interface.
 - For a high availability pair, enter the service IP address for the trusted interface.
- Step 5** Enter a Model Name and Software Version, as necessary.
- Step 6** For the Network Device Group, specify a Location and Device Type, as necessary.
- Step 7** Check the **Authentication Settings** check box, and enter the RADIUS shared secret information.
- Step 8** Click **Save**.
-

Remove an Inline Posture Node from Deployment

To remove an Inline Posture node from a deployment, you must first change its deployment to maintenance mode and then deregister it. Maintenance mode is a neutral state that allows the node to smoothly transition to the network or from a deployment.

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 check box next to the Inline Posture node that you want to remove from the deployment, and click **Edit**.
 - Step 3** Click the **Deployment Modes** tab.
 - Step 4** Click the **Maintenance Mode** radio button, and then click **Save**.
 - Step 5** Click **Deployment** on the left pane, and then check the check box next to the Inline Posture node that you want to remove from the deployment.
 - Step 6** Click **Deregister**.
 - Step 7** Click **OK**.
-

Health of an Inline Posture Node

You can monitor the health of a deployed Inline Posture node from the Cisco ISE dashboard that is running on the Administration node. The Inline Posture node appears on the System Summary dashlet. A green icon with a check mark means that the system is healthy. A yellow icon indicates a warning, and a red icon indicates a critical system failure. Sparklines indicate the utilization of CPU, memory, and latency over time. You can choose to display data for the past 24 hours or the last 60 minutes.

When you hover your mouse cursor over the health icon, a quick view dialog appears showing detailed information on system health.

Figure 16: System Summary Quick View Status

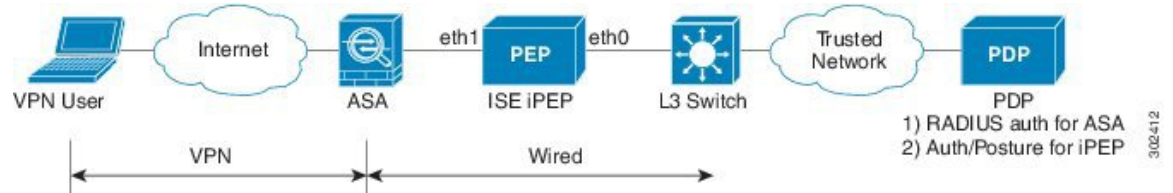
Name	Utilization and Latency 24h		
	CPU	Memory	Latency
<input checked="" type="checkbox"/> HAREESH-R6-			
<input checked="" type="checkbox"/> HAREESH-R6-			
<input checked="" type="checkbox"/> Inline Posture Service: up			

Remote Access VPN Use Case

This section describes how to use an Inline Posture node with a VPN device such as ASA in a Cisco ISE network. The following figure shows a Cisco ISE deployment that uses an Inline Posture node for remote VPN access. The term iPEP in this illustration refers to the Inline Posture node and PDP refers to the Policy

Service node. All the traffic from the VPN gateway must go through the Inline Posture node to ensure that Cisco ISE can apply policies and secure a network.

Figure 17: Cisco ISE Deployment with Inline Posture Node



Process Flow

- 1 Remote user authenticates to VPN gateway (ASA) using the RADIUS protocol.
- 2 As a RADIUS client, the ASA sends an authentication request to the AAA server (Inline Posture node).
- 3 As a RADIUS proxy, the Inline Posture node relays the RADIUS authentication request to the Cisco ISE node that acts as the RADIUS Server (Policy Service node).
- 4 The Cisco ISE Policy Service node authenticates the remote user using the configured identity store and returns the RADIUS response to the Inline Posture node which in turn relays it to the ASA (the network access device (NAD)).
- 5 Based on the authorization policy that is applicable for the user, the Policy Service node returns the appropriate attributes to the Inline Posture node and, optionally, to the ASA.
- 6 Each authorization policy rule entry can reference separate authorization profiles for both the Inline Posture node profile and the NAD (standard authorization profile).

Inline Posture node profile: Specifies RADIUS attributes to be applied to the Inline Posture node such as a URL for redirection to the Client Provisioning service and downloadable access control lists (DACLS) for policy enforcement by the Inline Posture node.

Standard authorization profile: Specifies any RADIUS attributes intended for the NAD, which is ASA in this example.

- 7 If the authorization policy determines that the endpoint is NonCompliant with the posture policy, or if the posture status is Unknown, then the Policy Service node returns a URL redirect attribute value to the Inline Posture node along with a DACL to specify the traffic to be allowed. All HTTP/HTTPS traffic denied by the DACL is redirected to the specified URL.
- 8 When the posture becomes Compliant, a reauthorization occurs and the Policy Service node sends a new DACL to the Inline Posture node, which provides the user privileged access to the internal network.

Configure an Inline Posture Node with a VPN Device

Before You Begin

Ensure that your network infrastructure is configured correctly to route or switch traffic to and from the Inline Posture node and its downstream networks.

-
- Step 1** Configure a standalone Cisco ISE node.
 - Step 2** Register the standalone Cisco ISE node as an Inline Posture node to an existing PAN, and configure the Inline Posture node from the PAN.
 - Step 3** Optionally, you can configure a second Inline Posture node and configure an Active/Standby pair.
 - Step 4** Set up a Policy Service node to be the RADIUS server for the Inline Posture node. Configure the Policy Service node with the same RADIUS shared secret that is configured on the Inline Posture node.
 - Step 5** Configure authorization profiles (Inline Posture node profiles) for use by the Inline Posture node.
 - Step 6** (Optional) You can configure standard authorization profiles for the NAD's use.
 - Step 7** Configure an authorization policy to apply the Inline Posture node profiles to remote VPN users based on identity and posture status.
 - Step 8** Add the VPN gateway's inside IP address as a RADIUS client in the Inline Posture node's RADIUS configuration along with the NAD's (ASA in this example) RADIUS shared secret.
 - Step 9** Configure the VPN gateway (ASA) for RADIUS authentication and accounting with the Inline Posture node configured as the RADIUS server. To do this:
 - a) Choose **Policy > Authentication**.
 - b) Ensure that the Default Rule is configured to authenticate users against the identity source that contains the user records.
 - c) Click **Save**.
-

Collection of Inline Posture Node Logs

From the Inline Posture node CLI, all the logs can be archived and collected using the backup-logs command.

```
PEP/admin# config terminal
PEP/admin# repository remoteloc
PEP/admin# url ftp://myremoteserver/store
PEP/admin# user <myremoteuser> password plain <myremotepasswd>
PEP/admin# end
PEP/admin# backup-logs myipeplogs repository remoteloc
% Creating log backup with timestamped filename: myipeplogs-110317-1836.tar.gz
```



Note

Collecting Inline Posture node logs remotely from the Primary Administration UI is not supported.

Kclick process in Inline Posture Node

Kclick kernel module process, called as kclick owns CPU scheduling in Inline Posture node. Kclick provides the CPU cycles for other processes that request it. Due to this the 'top' output at an Inline Posture Node displays the kclick using all the CPU cycles in the system including idle cycles.



PART

Setup Cisco ISE Management Access

- [Administer Cisco ISE, page 99](#)
- [Manage Administrators and Admin Access Policies, page 113](#)
- [Cisco ISE Licenses, page 133](#)
- [Manage Certificates, page 141](#)
- [Manage Network Devices, page 185](#)
- [Manage Resources, page 211](#)
- [Logging Mechanism, page 215](#)
- [Backup and Restore Operations, page 227](#)
- [Setup Endpoint Protection ServiceAdaptive Network Control, page 245](#)



Administer Cisco ISE

- [Log in to Cisco ISE, page 99](#)
- [Specify Proxy Settings in Cisco ISE, page 100](#)
- [Ports Used by the Admin Portal, page 101](#)
- [Specify System Time and NTP Server Settings, page 101](#)
- [Change the System Time Zone, page 102](#)
- [Configure SMTP Server to Support Notifications, page 103](#)
- [Install a Software Patch, page 103](#)
- [Roll Back Software Patches, page 105](#)
- [View Patch Install and Rollback Changes, page 106](#)
- [FIPS Mode Support, page 106](#)
- [Enable FIPS Mode in Cisco ISE, page 107](#)
- [Configure Cisco ISE for Administrator CAC Authentication, page 108](#)
- [Securing SSH Key Exchange Using Diffie-Hellman Algorithm, page 110](#)
- [Configure Cisco ISE to Send Secure Syslog, page 110](#)

Log in to Cisco ISE

Log in to Cisco ISE using your administrator username and password.

During the initial setup, if you do not enable SSH then you will not be able to access the ISE admin console via SSH. To enable SSH, enter the **service sshd enable** command in the global configuration mode, by

accessing the Cisco ISE CLI. You can disable SSH by using the **no service sshd** command in the global configuration mode.

-
- 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.
-

Administrator Login Browser Support

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

- Mozilla Firefox versions 31.x ESR, 36.x, and 37.x
- Mozilla Firefox versions 31.x ESR, 32.x, and 33.x
- Microsoft Internet Explorer 10.x and 11.x

Adobe Flash Player 11.2.0.011.1.0.0 or above must be installed on the system running your client browser.

The minimum required screen resolution to view the Admin portal and for a better user experience is 1280*800 pixels.

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

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.

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.

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 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** 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:
- Click **Add**.
 - 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.
 - Return to the NTP Server Configuration tab when you are finished entering the NTP Server Authentication Keys.
- Step 5** Click **Save**.
-

Change 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** 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 3** 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 4** 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>`.

Install a Software Patch

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



Note Cisco ISE allows you to install a patch on an Inline Posture node only through the CLI.

To install patches from the CLI, refer to *Cisco Identity Services Engine CLI Reference Guide*.

Before You Begin

- You must have the Super Admin or System Admin administrator role assigned.
- Make sure that the auto-failover configuration, if enabled in your deployment, is turned off. When you install a software patch, 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 > 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.

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.

Software Patch Installation Guidelines

When you install or roll back a patch from a standalone or Primary Administration Node (PAN), Cisco ISE restarts the application. You might have to wait for a few minutes before you can log in again.

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 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 PAN, Cisco ISE then continues patch installation on the secondary nodes. If it fails on the 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. Secondary Cisco ISE nodes are restarted consecutively after the patch is installed on those nodes. While installing a patch on secondary nodes, you can continue to perform tasks on the PAN.

Roll Back Software Patches

When you roll back a patch from the PAN that is part of a distributed deployment, 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.
- Make sure that the auto-failover configuration, if enabled in your deployment, is turned off. When you roll back a software patch, 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 > 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 any secondary nodes 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.

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

The monitoring and troubleshooting component of Cisco ISE provides information on the patch installation and rollback operations that are performed on your Cisco ISE nodes according to a time period that you specify.

Before You Begin

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

-
- Step 1** Choose **Operations** > **Reports** > **Catalog** > **Server Instance**.
 - Step 2** Click the **Server Operations Audit** radio button, click **Run**, and choose the time period for which you want to generate the report.
 - Step 3** Click the **Launch Interactive Viewer** link in the upper right corner of the page to view, sort, and filter the data in this report.
-

FIPS Mode Support

Product Cisco Identity Services Engine uses embedded FIPS 140-2 validated cryptographic modules Cisco Common Cryptographic Module (Certificate #1643 and #2100). For details of the FIPS compliance claims, see the [FIPS Compliance Letter](#).

When FIPS mode is enabled, the Cisco ISE administrator interface displays a FIPS mode icon to 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 level 1 standard, Cisco ISE displays a warning with the name of the protocol or certificate that is noncompliant, and FIPS mode will not be enabled. Ensure that you choose only FIPS-compliant protocols and replace non-FIPS-compliant certificates before you enable FIPS mode.

After you enable 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 Administration Node (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.

Cisco ISE, Release 1.3, does not support FIPS mode.

Enable FIPS Mode in Cisco ISE

You can provide Federal Information Processing Standard (FIPS) 140-2 compliant encryption and decryption in your Cisco ISE network.

-
- 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

Once you have enabled FIPS mode, enable and configure the following FIPS 140-2 compliant functions:

- [Import Network Devices into Cisco ISE](#), on page 187
- [Generate a Self-Signed Certificate](#), on page 149
- [Create a Certificate Signing Request and Submit the CSR to a Certificate Authority](#), on page 157
- Configure RADIUS authentication settings under [Network Device Definition Settings](#), on page 729.

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.

FIPS Mode Operational Parameters

The FIPS standard places limitations on the use of certain algorithms. In order to enforce this standard, you must enable FIPS operation in Cisco ISE. Cisco ISE enables FIPS 140-2 compliance via RADIUS shared secret and key management measures. While in FIPS mode, any functions using non-FIPS-compliant algorithms fail, and certain authentication functionality is disabled.

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.

Cisco NAC Agent Requirements when FIPS Mode is Enabled

The Cisco NAC Agent always looks for the Windows Internet Explorer TLS 1.0 settings to discover the Cisco ISE network. (These TLS 1.0 settings should be enabled in Internet Explorer.) Therefore, client machines must have Windows Internet Explorer Version 7, 8, or 9 installed and TLS1.0 enabled to allow for Cisco ISE posture assessment functions to operate on client machines accessing the network. The Cisco NAC Agent can automatically enable the TLS 1.0 setting in Windows Internet Explorer if FIPS mode has been enabled in Cisco ISE.

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.
- Click **Browse** to choose the certificate.
 - Check the Trust for client authentication check box.
 - 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.
- Choose **Administration > System > Certificates > OSCP Services**.
 - Enter the name of an OSCP server, an optional description, and the URL of the server.
 - Choose **Administration > System > Certificates > Certificate Store**.
 - 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**.
- Choose Client Certificate Based authentication type on the Authentication Method tab.
 - Choose the certificate authentication profile that you configured earlier.
 - Select the Active Directory instance name.
 - 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.
-

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 <http://www.actividentity.com/products/securityclients/ActivClient/>.

Common Access Card Operation in Cisco ISE

The Admin portal can be configured so that you 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:

```
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 Administration Node (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.
-

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.
- Enter the buffer size.
 - 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
 - Posture and Client Provisioning 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.
-



CHAPTER 6

Manage Administrators and Admin Access Policies

- [Role-Based Access Control](#), page 113
- [Cisco ISE Administrators](#), page 113
- [Cisco ISE Administrator Groups](#), page 114
- [Administrative Access to Cisco ISE](#), page 121

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 administrators (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.

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.
-

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.

Read-only functionality is unavailable for any administrative access in Cisco ISE. 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

Admin Group Role	Access Level	Permissions	Restrictions
Customization Admin	Manage sponsor, guest, and personal devices portals	<ul style="list-style-type: none"> • Configure guest and sponsor access. • Manage guest access settings. • Customize end-user web portals. 	<ul style="list-style-type: none"> • Cannot perform any policy management or identity management or system-level configuration tasks in Cisco ISE • Cannot view any reports
Helpdesk Admin	Query monitoring and troubleshooting operations	<ul style="list-style-type: none"> • Run all reports • Run all troubleshooting flows • View the Cisco ISE dashboard and livelogs • View alarms 	Cannot create, update, or delete reports, troubleshooting flows, live authentications, or alarms

Admin Group Role	Access Level	Permissions	Restrictions
Identity Admin	<ul style="list-style-type: none"> • Manage user accounts and endpoints • Manage identity sources 	<ul style="list-style-type: none"> • Add, edit, and delete user accounts and endpoints • Add, edit, and delete identity sources • Add, edit, and delete identity source sequences • Configure general settings for user accounts (attributes and password policy) • View the Cisco ISE dashboard, livelogs, alarms, and reports. • Run all troubleshooting flows. 	Cannot perform any policy management or system-level configuration tasks in Cisco ISE
MnT Admin	Perform all monitoring and troubleshooting operations.	<ul style="list-style-type: none"> • Manage all reports (run, create, and delete) • Run all troubleshooting flows • View the Cisco ISE dashboard and livelogs • Manage alarms (create, update, view, and delete) 	Cannot perform any policy management or identity management or system-level configuration tasks in Cisco ISE

Admin Group Role	Access Level	Permissions	Restrictions
Network Device Admin	Manage Cisco ISE network devices and network device repository.	<ul style="list-style-type: none"> • 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 	Cannot perform any policy management or identity management or system-level configuration tasks in Cisco ISE
Policy Admin	Create and manage policies for all Cisco ISE services across the network that are related to authentication, authorization, posture, profiler, client provisioning.	<ul style="list-style-type: none"> • 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 	Cannot perform any identity management or system-level configuration tasks in Cisco ISE

Admin Group Role	Access Level	Permissions	Restrictions
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	<ul style="list-style-type: none"> • 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

Admin Group Role	Access Level	Permissions	Restrictions
Super Admin	All Cisco ISE administrative functions. The default administrator account belongs to this group.	<p>Create, read, update, delete, and eXecute (CRUDX) permissions on all Cisco ISE resources.</p> <p>Note 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.</p>	

Admin Group Role	Access Level	Permissions	Restrictions
System Admin	All Cisco ISE configuration and maintenance tasks.	<p>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.</p> <ul style="list-style-type: none"> • 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 • 	Cannot perform any policy management or system-level configuration tasks in Cisco ISE
External RESTful Services (ERS) Admin	Full access to all ERS API requests such as GET, POST, DELETE, PUT	<ul style="list-style-type: none"> • 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

Admin Group Role	Access Level	Permissions	Restrictions
External RESTful Services (ERS) Operator	Read-only access to ERS API, only GET	<ul style="list-style-type: none"> • Can only Read ERS API requests 	The role is meant only for ERS authorization supporting Internal Users, Identity Groups, Endpoints, Endpoint Groups, and SGT

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.
-

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 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, 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.

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. The following table lists the default menu access permissions. 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.

Table 5: Default Menu Access Permissions

Menu Access Name	RBAC Group	Permissible Set of Menu Items
Super Admin Menu Access	Super Admin	Operations > All menu items Policy > All menu items Administration > All menu items
Policy Admin Menu Access	Policy Admin	Operations > All menu items Policy > All menu items Administration > Identity Management > All menu items System > Settings
Helpdesk Admin Menu Access	Helpdesk Admin	Operations > All menu items
Identity Admin Menu Access	Identity Admin	Operations > All menu items Administration > Identity Management > All menu items
Network Device Menu Access	Network Device Admin	Operations > All menu items Administration > Network Resources > All menu items
System Admin Menu Access	System Admin	Operations > Authentications, Alarms, Reports, and Troubleshoot Administration > System > All menu items
RBAC Admin Menu Access	RBAC Admin	Operations > All menu items except Endpoint Protection Services Adaptive Network Control Administration > Admin Access > All menu items
MnT Admin Menu Access	MnT Admin	Operations > All menu items

**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.
- Click to expand the menu item up to the desired level, and click the menu item(s) on which you want to create permissions.
 - In the Permissions for Menu Access area, click **Show**.
- Step 3** Click **Submit**.
-

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. The following table lists the default data access permissions. 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.

Table 6: Default Data Access Permissions

Data Access Name	RBAC Group	Permissible Admin Groups	Permissible Network Device Groups
Super Admin Data Access	Super Admin	Admin Groups, User Identity Groups, Endpoint Identity Groups	All Locations, All Device Types
Policy Admin Data Access	Policy Admin	User Identity Groups, Endpoint Identity Groups	None
Identity Admin Data Access	Identity Admin	User Identity Groups, Endpoint Identity Groups	None
Network Admin Data Access	Network Device Admin	None	All Locations, All Device Types

Data Access Name	RBAC Group	Permissible Admin Groups	Permissible Network Device Groups
System Admin Data Access	System Admin	Admin Groups	None
RBAC Admin Data Access	RBAC Admin	Admin Groups	None

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.
- Click to expand the admin group and select the desired admin group.
 - Click **Full Access**.
- Step 4** Click **Save**.
-

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 contains a list of default policies. These default policies cannot be modified or deleted. This page also allows you to create custom RBAC policies for an admin group specifically for your work place, and apply to personalized admin groups.

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.
- 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**.
-

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. These restrictions are not applicable for the Inline Posture 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** From the Configure IP List for Access Restriction area, click **Add**.
 - Step 3** Enter IP addresses in the classless interdomain routing (CIDR) format in the IP address field.
 - Step 4** Enter the subnet mask in the Netmask in CIDR format field.
 - Step 5** Click **OK**. Repeat the process to add more IP address ranges to this list.
 - Step 6** Click **Save** to save the changes.
-

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.

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 > Add**.
- Step 2** Enter a name and optional description.
- Step 3** 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 4** 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 5** Click **Save**.
-

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:
- **Menu Access**—All administrators who belong to the external administrator group can be granted permission at the menu or submenu level. The menu access permission determines the menus or submenus that they can access.
 - **Data Access**—All administrators who belong to the external administrator group can be granted permission at the data level. The data access permission determines the data that they can access.
- Step 3** Specify menu access or data access permissions for the external administrator group.
- Step 4** Click **Save**.
-

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**.
-



Cisco ISE Licenses

This chapter describes the licensing mechanism and schemes that are available for Cisco ISE and how to add and upgrade licenses.

- [Cisco ISE Licenses, page 133](#)
- [License Consumption, page 135](#)
- [Manage License Files, page 137](#)

Cisco ISE Licenses

Cisco ISE licensing provides the ability to manage the application features and access, such as the number of concurrent endpoints that can use Cisco ISE network resources.

To maximize economy for customers, licensing in Cisco ISE is supplied in different packages as Base, Plus, Apex, and Mobility Upgrade.

All Cisco ISE appliances are supplied with a 90-day Evaluation license. 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 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 primary Administration node, you must obtain a license for Cisco ISE and then register that license. You register all licenses to the Cisco ISE primary Administration node via the primary and secondary Administration node hardware UID. The primary Administration node then centrally manages all the licenses that are registered for your deployment.

Cisco recommends installing both Base and Plus or Apex licenses at the same time.

- Using a Plus or Apex license requires also using a Base license. 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.

- You cannot upgrade the Evaluation license to an Plus and/or Apex license without first installing the Base license.
- Cisco ISE allows you to use more Plus and/or Apex licenses on the system than Base licenses. For example, you can have 100 Base licenses and Plus licenses.
- When you install a Mobility Upgrade license, Cisco ISE enables all Wired, Wireless, and VPN services.

Table 7: Cisco ISE License Packages

ISE License Packages	Perpetual/Subscription (Terms Available)	ISE Functionality Covered	Notes
Base	Perpetual	<ul style="list-style-type: none"> • Basic network access: AAA, IEEE-802.1X • Guest management • Link encryption (MACSec) • TrustSec • ISE Application Programming Interfaces 	
Plus	Subscription (1, 3, or 5 years)	<ul style="list-style-type: none"> • Bring Your Own Device (BYOD) with built-in Certificate Authority Services • Profiling and Feed Services • Endpoint Protection Service (EPS) • Cisco pxGrid 	Does not include Base services; a Base license is required to install the Plus license.
Apex	Subscription (1, 3, or 5 years)	<ul style="list-style-type: none"> • Third Party Mobile Device Management (MDM) • Posture Compliance 	Does not include Base services; a Base license is required to install the Apex license.
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, 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.
Evaluation	Temporary (90 days)	Full Cisco ISE functionality is provided for 100 endpoints.	All Cisco ISE appliances are supplied with an Evaluation license.

License Consumption

You purchase licenses for the number of concurrent users on the system. 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.
- A Plus license turns on the pxGrid feature. This feature does not consume licenses.
- 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.

View License Consumption

You can view your system's current license consumption from the Licensing dashboard at: **Administration > System > Licensing**. 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 > Authorization**, identify the 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 137](#)
- [Re-Host Licenses, on page 137](#)
- [Renew Licenses, on page 138](#)
- [Migrate and Upgrade Licenses, on page 138](#)
- [Remove Licenses, on page 138](#)

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, 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 the Licensing dashboard **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, 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. Existing Wireless/Wireless Upgrade deployment will be migrated to Mobility/Mobility Upgrade package during upgrade from Cisco ISE version 1.2 to 1.3. You can also purchase bundles of licenses to minimize your ongoing expenses. These scenarios are all covered in the [licensing site](#), 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.



Note

After upgrading from Cisco ISE version 1.2, 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**.



CHAPTER 8

Manage Certificates

- [Certificate Management in Cisco ISE, page 141](#)
- [Cisco ISE CA Service, page 165](#)
- [OCSP Services, page 181](#)

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.

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
- 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.

Certificate Matching in Cisco ISE

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.

**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, which is a system certificate along with the sequence of trust certificates that sign it, can be imported, subject to certain restrictions.

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 service.

By default, a Cisco ISE node is preinstalled with a self-signed certificate that is used for EAP, Admin, Portal, and pxGrid services. 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 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`.

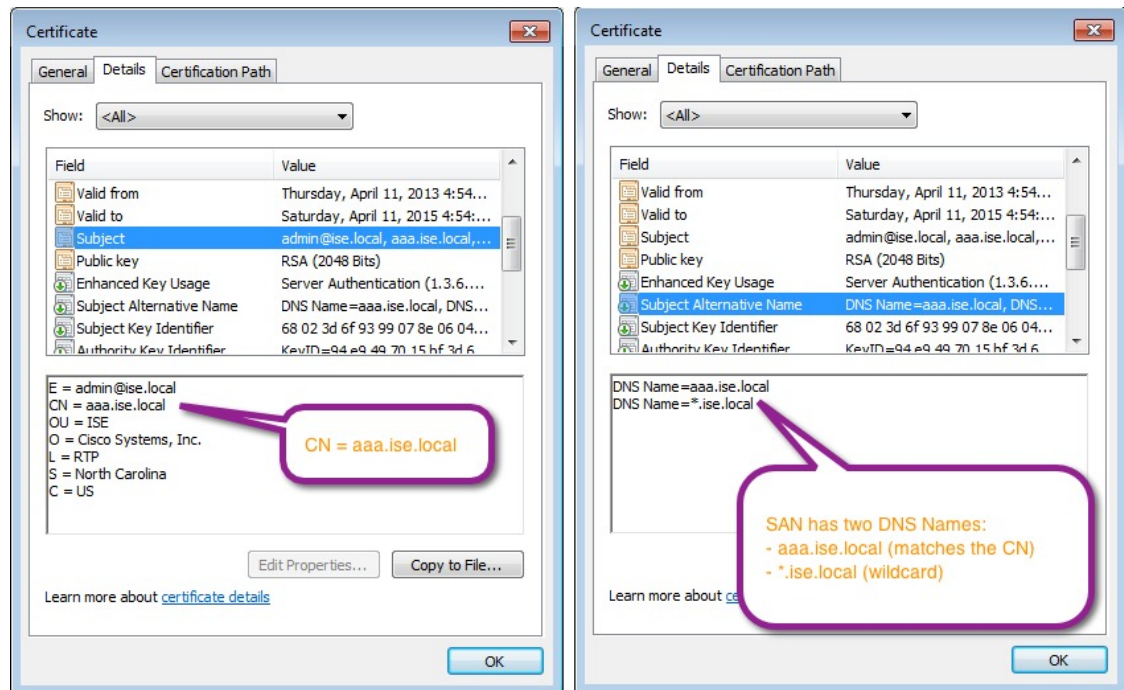
If you configure a wildcard certificate to use `*.ise.local`, you can use the same certificate to secure any other host whose DNS name ends with `“.ise.local,”` such as:

- `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.

Figure 18: Wildcard Certificate Example



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.



Note

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 example, SessionIdValue is replaced with the actual session ID of the request. 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.

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 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, a self-signed certificate is created on a Cisco ISE node during installation time, and this certificate is designated for EAP, Admin, Portal, and pxGrid use (it has a key length of 1024 and is valid for one year).


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

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 Enter the values for the certificate that you are going to import.

Step 3 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** 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.
- Step 4** Check the check boxes 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 **Renew Self Signed Certificate** 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.

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 used for Admin, EAP Authentication, Portals, or pxGrid service. 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.

-
- Step 1** Choose **Administration > System > Certificates > System Certificates**.
 - Step 2** Check the check boxes 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 check box 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 the 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 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.

Certificates in Trusted Certificates Store

The Trusted Certificate Store is prepopulated with trusted certificates: Manufacturing certificate, Root certificate, Endpoint CA, Endpoint RA, 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
  DirName: C = BE, ST = EMEA, L = BN, O = ABCDE Group, OU = Domestic
```

```

DirName: C = CH, ST = EMEA, L = CH, O = ABCDE Group, OU = Service Z100
URI:.dir
IP:172.23.0.171/255.255.255.255
Excluded:
DNS:.dir
URI:.dir

```

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 **Administration > System > Certificates > Trusted Certificates**. The Trusted Certificates page appears, listing all the trusted certificates.

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 check box 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** check box 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 in to 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 688 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 **Allow Wildcard Certificates** check box to bind a certificate that contains the wildcard character, asterisk (*) in any CN in the Subject or DNS in the Subject Alternative Name.
- Step 6** Check the **Enable Validation of Certificate Extensions** check box if you want Cisco ISE to validate certificate extensions. If you enable the **Enable Validation of 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.
- Step 7** 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 8** 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 156](#)

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 157](#)
- Step 2** [Import the Root Certificates to the Trusted Certificate Store, on page 156](#)
- Step 3** [Bind the CA-Signed Certificate to the CSR, on page 158](#)
-

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.

-
- Step 1** [Create a Certificate Signing Request and Submit the CSR to a Certificate Authority, on page 157.](#)
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 156.](#)
- Step 3** [Bind the CA-Signed Certificate to the CSR, on page 158.](#)
-

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:

Step 1 Create a self-signed certificate, choose "Portal" as a service, and assign a different certificate group tag (for example, tempportaltag).

Step 2 Change the portal configuration to use the newly created certificate group tag (tempportaltag).

Step 3 Edit the default self-signed certificate and remove the Portal role.
This option removes the Default Portal Certificate Group tag association with the default self-signed certificate.

Step 4 Do one of the following:

Option	Description
Generate a CSR	<p>When you generate the CSR:</p> <ol style="list-style-type: none"> 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 in to the Trusted Certificates store. 4 Bind the CA-signed certificate with the CSR.
Import the private key and the CA-signed certificate	<p>When you import the CA-signed certificate:</p> <ol style="list-style-type: none"> 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 in to the Trusted Certificates store.

Option	Description
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 163](#)
 - Step 2** [Create an Authorization Policy Profile for CWA Redirection, on page 164](#)
 - Step 3** [Create an Authorization Policy Rule to Renew Certificates, on page 164](#)
-

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 164](#)

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**.
-



Note

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 EQUALS Guest Flow) and Profile = Wireless-Permit

What to Do Next

[Create an Authorization Policy Rule to Renew Certificates, on page 164](#)

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 **Policy > 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.

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

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. The ISE CA offers the following functionalities:

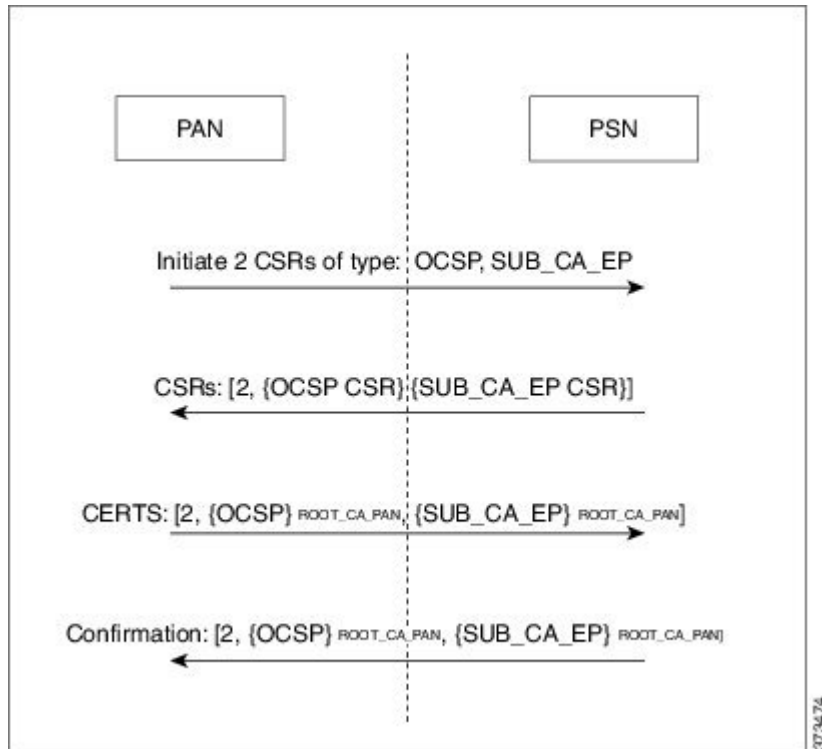
- **Certificate Issuance:** Validates and signs Certificate Signing Requests (CSRs) for endpoints that connect to your network.
- **Key Management:** Generates and securely stores keys and certificates on both PAN and PSN nodes.
- **Certificate Storage:** Stores certificates issued to users and devices.
- **Online Certificate Status Protocol (OCSP) Support:** Provides an OCSP responder to check for the validity of certificates.

Certificates Provisioned on Primary Administration Node and Policy Service Nodes

After installation, a Cisco ISE node is provisioned with self-signed CA and subordinate CA (sub CA) certificates for the Cisco ISE node to issue and manage certificates for endpoints. Any PSN that you register with your PAN is provisioned with a sub CA certificate that is signed by the PAN. When you use the Cisco ISE internal

CA service and endpoints access your network, then the sub CA on the PSN node issues certificates to endpoints.

Figure 19: Certificates Provisioned At Node Registration - PSNs get an Endpoint CA and an OCSP certificates from the PAN



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.

For details on how to set up your Microsoft SCEP server to interoperate with Cisco ISE, see

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf.

Endpoint Certificates

The Admin portal lists all the certificates issued by the internal ISE CA to endpoints (Administration > System > Certificates > Endpoint Certificates). The Endpoint 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 , Subject, Subject Alternative Name (SAN), and Validity of the certificate. You can click on the endpoint certificate to view the certificate.

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.

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 in to 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 OCSF Responder Certificate of ise-vm1
Issuer:CN=Cisco ISE Self-Signed CA of ise-vm1
Serial#:0x5082017f-330e412f-8d63305d-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 PAN and PSN

When you set up the deployment, Cisco ISE generates a root CA on the Primary Administration Node (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 PAN or PSN, you must regenerate root CA on the 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 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** Choose **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 Administration node in the deployment, obtain a backup of the Cisco ISE CA certificates and keys from the PAN and restore it on the secondary Administration node. This ensures that the secondary Administration node can function as the root CA in case of a PAN failure and you promote the secondary Administration node to be the PAN.

Configure Cisco ISE Root CA as Subordinate CA of an External PKI

If you want the root CA on the 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 in to the Trusted Certificates Store, and bind the CA-signed certificate to the CSR. In

this case, the external CA is the root CA, the PAN is a subordinate CA of the external CA, and the PSNs are subordinate CAs of the 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 Administration node in the deployment, obtain a backup of the Cisco ISE CA certificates and keys from the PAN and restore it on the secondary Administration node. This ensures that the secondary Administration node can function as subordinate CA of the external PKI in case of a PAN failure and you promote the secondary Administration node to be the 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 PAN and store them in a secure location for disaster recovery purposes.
- If you have a secondary Administration node in the deployment, back up the Cisco ISE CA certificates and keys from the PAN and restore them on the secondary Administration node.

-
- Step 1** [Add Users to the Employee User Group, on page 171](#)
You can add users to the internal identity store or to an external identity store such as Active Directory.
- Step 2** [Create a Certificate Authentication Profile for TLS-Based Authentication, on page 171](#)
- Step 3** [Create an Identity Source Sequence for TLS-Based Authentication, on page 172](#)
- Step 4** Creating a client provisioning policy.
- a) [Configure Certificate Authority Settings, on page 172](#)
 - b) [Create a CA Template, on page 173](#)
 - c) [Create a Native Supplicant Profile to be Used in Client Provisioning Policy, on page 174](#)
 - d) [Download Agent Resources from Cisco Site for Windows and MAC OS X Operating Systems, on page 175](#)

e) [Create Client Provisioning Policy Rules for Apple iOS, Android, and MACOSX Devices, on page 175](#)

Step 5 [Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication, on page 176](#)

Step 6 Configure authorization policy rules for TLS-based authentications.

- a) [Create Authorization Profiles for Central Web Authentication and Supplicant Provisioning Flows, on page 176](#)
- b) [Create Authorization Policy Rules, on page 177](#)

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.

Step 1 Choose **Administration > Identity Management > Identities > Users**.

Step 2 Click **Add**.

Step 3 Enter the user details.

Step 4 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 5 Click **Submit**.

What to Do Next

[Create a Certificate Authentication Profile for TLS-Based Authentication, on page 171](#)

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.

Step 1 Choose **Administration > Identity Management > External Identity Sources > Certificate Authentication Profile**.

Step 2 Enter a name for your certificate authentication profile. For example, CAP.

Step 3 Choose Subject - Common Name as the **Principal Username X509 Attribute**.

Step 4 Click **Save**.

What to Do Next

[Create an Identity Source Sequence for TLS-Based Authentication, on page 172](#)

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 1** Choose **Administration > Identity Management > Identity Source Sequences**.
- Step 2** Click **Add**.
- Step 3** Enter a name for the identity source sequence. For example, Dot1X.
- 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 172](#)

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 8: Device Certificate Location

Device	Certificate Storage Location	Access Method
iPhone/iPad	Standard certificate store	Settings > General > Profile

Device	Certificate Storage Location	Access Method
Android	Encrypted certificate store	Invisible to end users. Note Certificates can be removed using Settings > Location & Security > Clear Storage.
Windows	Standard certificate store	Launch mmc.exe from the /cmd prompt or view in the certificate snap-in.
Mac	Standard certificate store	Application > Utilities > Keychain Access

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 173](#)

Create a CA Template

The certificate template defines the SCEP RA profile that must be used (for the internal or external CA), , 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.

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 size. You must choose 1024 or a higher key size.
- Step 6** 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 7** 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 174](#)

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 8909 and UDP port 8909 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.
 - 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 175

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 175

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/or 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 in 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 176

Configure the Dot1X Authentication Policy Rule for TLS-Based Authentication

You must 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 > Authentication**.
 - Step 2** Click the Rule-Based radio button.
The default rule-based authentication policy includes a rule for Dot1X authentication.
 - Step 3** Edit the Dot1X authentication policy rule.
 - Step 4** Choose **Actions > Insert new row above** from the Dot1X policy rule.
 - Step 5** Enter a name for the rule. For example, eap-tls.
 - Step 6** Use the Expression Builder to create the following policy condition: If Network Access:EapAuthentication Equals EAP-TLS, then use the certificate authentication profile that you created earlier.
 - Step 7** Leave the default rule as is.
 - Step 8** Click **Save**.
-

What to Do Next

[Create Authorization Profiles for Central Web Authentication and Supplicant Provisioning Flows](#), on page 176

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 177](#)

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 > Authorization**.
- 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.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
iOS	Any	Apple iOS All	Condition(s)	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.
Android	Any	Android	Condition(s)	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.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
MACOSX	Any	MACOSX	Condition(s)	<p>Under the Native Supplicant Configuration, specify the following:</p> <ol style="list-style-type: none"> 1 Config Wizard: Select the MACOSX supplicant wizard that you downloaded from the Cisco site. 2 Wizard Profile: Choose the <code>EAP_TLS_INTERNAL</code> 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.

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=https://ip:port/blacklistportal/gateway?portal=PortalID
- 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.

Rule Name	Conditions	Permissions (authorization profiles to be applied)
Corporate Assets	Corp_Assets AND (Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	PermitAccess
Android_SingleSSID	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android)	NSP_Google
Android_DualSSID	(Wireless_MAB AND Session:Device-OS EQUALS Android)	CWA_GooglePlay
CWA	Wireless_MAB	CWA

Rule Name	Conditions	Permissions (authorization profiles to be applied)
NSP	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	NSP
EAP-TLS	(Wireless 802.1X AND Network Access:AuthenticationMethod EQUALS x509_PKI)	PermitAccess

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.

-
- 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* 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 9: OCSP Syslog Messages

Message	Description
OCSPPrimaryNotResponsiveCount	The number of nonresponsive primary requests
OCSPSecondaryNotResponsiveCount	The number of nonresponsive secondary requests
OCSPPrimaryCertsGoodCount	The number of 'good' certificates that are returned for a given CA using the primary OCSP server
OCSPSecondaryCertsGoodCount	The number of 'good' statuses that are returned for a given CA using the primary OCSP server
OCSPPrimaryCertsRevokedCount	The number of 'revoked' statuses that are returned for a given CA using the primary OCSP server
OCSPSecondaryCertsRevokedCount	The number of 'revoked' statuses that are returned for a given CA using the secondary OCSP server
OCSPPrimaryCertsUnknownCount	The number of 'Unknown' statuses that are returned for a given CA using the primary OCSP server
OCSPSecondaryCertsUnknownCount	The number of 'Unknown' statuses that are returned for a given CA using the secondary OCSP server
OCSPPrimaryCertsFoundCount	The number of certificates that were found in cache from a primary origin
OCSPSecondaryCertsFoundCount	The number of certificates that were found in cache from a secondary origin
ClearCacheInvokedCount	How many times clear cache was triggered since the interval
OCSPCertsCleanedUpCount	How many cached entries were cleaned since the t interval
NumOfCertsFoundInCache	Number of the fulfilled requests from the cache
OCSPCacheCertsCount	Number of certificates that were found in the OCSP cache



Manage Network Devices

- [Network Devices Definitions in Cisco ISE, page 185](#)
- [Default Network Device Definition in Cisco ISE, page 186](#)
- [Create a Network Device Definition in Cisco ISE, page 187](#)
- [Import Network Devices into Cisco ISE, page 187](#)
- [Export Network Devices from Cisco ISE, page 188](#)
- [Network Device Groups, page 188](#)
- [Import Network Device Groups in to Cisco ISE, page 189](#)
- [Export Network Device Groups from Cisco ISE, page 190](#)
- [Import Templates in Cisco ISE, page 190](#)
- [Mobile Device Manager Interoperability with Cisco ISE, page 195](#)
- [Set Up MDM Servers With Cisco ISE, page 201](#)

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 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 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 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 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 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 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 request from a network device.

Cisco ISE performs the following procedure when a RADIUS 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 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 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.

-
- Step 1** Choose **Administration > Network Resources > Network Devices**.
 - Step 2** Click **Add**.
 - Step 3** Enter the required information in the **Network Devices** section.
 - Step 4** Check the **Authentication Settings** check box to configure RADIUS protocol for authentication.
 - Step 5** (Optional) Check the **SNMP Settings** check box to configure the Simple Network Management Protocol for the Profiling service to collect device information.
 - Step 6** (Optional) Check the **Advanced Trustsec Settings** check box to configure a Trustsec-enabled device.
 - Step 7** Click **Submit**.
-

Related Topics

[Network Devices Definitions in Cisco ISE, on page 185](#)

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 this back in to 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.

-
- 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.
- 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**.
-

Related Topics

- [Export Network Devices from Cisco ISE, on page 188](#)
- [Network Devices Import Template Format, on page 191](#)

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.

-
- 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.
-

Related Topics

- [Import Network Devices into Cisco ISE, on page 187](#)

Network Device Groups

Cisco ISE allows you to create hierarchical Network Device Groups (NDGs) that contain network devices. NDGs logically group network devices based on various criteria such as geographic location, device type, and the relative place in the network (like “Access Layer” or “Data Center,” for example).

For example, to organize your network devices by geographic location, you can group them by continent, region, and country:

- Africa -> Southern -> Namibia
- Africa -> Southern -> South Africa
- Africa -> Southern -> Botswana

You can also group network devices by 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 passes through 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.

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 also create a root Network Device Group (NDG), and then create child NDGs under the root group in the Network Device Groups page. When you create a new root NDG, you must provide the name and type of the NDG. This information is not required when you create a child under the root NDG.

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 in to 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.
-

Related Topics

[Import Network Device Groups into Cisco ISE](#)

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.

Related Topics

- [Import Network Devices into Cisco ISE, on page 187](#)
- [Export Network Devices from Cisco ISE, on page 188](#)
- [Import Network Device Groups into Cisco ISE](#)
- [Export Network Device Groups from Cisco ISE, on page 190](#)
- [Network Devices Import Template Format, on page 191](#)
- [Network Device Groups Import Template Format, on page 194](#)

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 10: CSV Template Fields and Description for Network Devices

Field	Description
Name:String(32):	(Required) This field is the network device name. It is an alphanumeric string, with a maximum of 32 characters in length.
Description:String(256)	This field is an optional description for the network device. A string, with a maximum of 256 characters in length.
IP Address:Subnets(a.b.c.d/m ...)	(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 “ ” symbol).
Model Name:String(32):	(Required) This field is the network device model name. It is a string, with a maximum of 32 characters in length.
Software Version:String(32):	(Required) This field is the network device software version. It is a string, with a maximum of 32 characters in length.
Network Device Groups:String(100):	(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
Authentication:Protocol:String(6)	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).
Authentication:Shared Secret:String(128)	(Required, if you enter a value for the Authentication Protocol field) This field is a string, with a maximum of 128 characters in length.

Field	Description
EnableKeyWrap:Boolean(true false)	This is an optional field. It is enabled only when it is supported on the network device. Valid value is true or false.
EncryptionKey:String(ascii:16 hexa:32)	(Required, if you enable KeyWrap) Indicates the encryption key that is used for session encryption. ASCII—16 characters (bytes) long Hexadecimal—32 characters (bytes) long.
AuthenticationKey:String(ascii:20 hexa:40)	(Required, if you enable KeyWrap). Indicates the keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages. ASCII—20 characters (bytes) long Hexadecimal—40 characters (bytes) long.
InputFormat:String(32)	Indicates encryption and authentication keys input format. Valid value is ASCII or Hexadecimal.
SNMP:Version:Enumeration (2c 3)	This is an optional field, used by the Profiler service. It is the version of the SNMP protocol. Valid value is 1, 2c, or 3.
SNMP:RO Community:String(32)	(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.
SNMP:RW Community:String(32)	(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.
SNMP:Username:String(32)	This is an optional field. It is a string, with a maximum of 32 characters in length.
SNMP:Security Level:Enumeration(Auth No Auth Priv)	(Required if you choose SNMP version 3) Valid value is Auth, No Auth, or Priv.
SNMP:Authentication Protocol:Enumeration(MD5 SHA)	(Required if you have entered Auth or Priv for the SNMP security level) Valid value is MD5 or SHA.
SNMP:Authentication Password:String(32)	(Required if you have entered Auth for the SNMP security level) It is a string, with a maximum of 32 characters in length.
SNMP:Privacy Protocol:Enumeration(DES AES128 AES192 AES256 3DES)	(Required if you have entered Priv for the SNMP security level) Valid value is DES, AES128, AES192, AES256, or 3DES.

Field	Description
SNMP:Privacy Password:String(32)	(Required if you have entered Priv for the SNMP security level) It is a string, with a maximum of 32 characters in length.
SNMP:Polling Interval:Integer:600-86400 seconds	This is an optional field to set the SNMP polling interval. Valid value is an integer between 600 and 86400.
SNMP:Is Link Trap Query:Boolean(true false)	This is an optional field to enable or disable the SNMP link trap. Valid value is true or false.
SNMP:Is MAC Trap Query:Boolean(true false)	This is an optional field to enable or disable the SNMP MAC trap. Valid value is true or false.
SNMP:Originating Policy Services Node:String(32)	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.
Trustsec:Device Id:String(32)	This is an optional field. It is the Trustsec device ID, and is a string, with a maximum of 32 characters in length.
Trustsec:Device Password:String(256)	(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.
Trustsec:Environment Data Download Interval:Integer:1-2147040000 seconds	This is an optional field. It is the Trustsec environment data download interval. Valid value is an integer between 1 and 24850.
Trustsec:Peer Authorization Policy Download Interval:Integer:1-2147040000 seconds	This is an optional field. It is the Trustsec peer authorization policy download interval. Valid value is an integer between 1 and 24850.
Trustsec:Reauthentication Interval:Integer:1-2147040000 seconds	This is an optional field. It is the Trustsec reauthentication interval. Valid value is an integer between 1 and 24850.
Trustsec:SGACL List Download Interval:Integer:1-2147040000 seconds	This is an optional field. It is the Trustsec SGACL list download interval. Valid value is an integer between 1 and 24850.
Trustsec:Is Other Trustsec Devices Trusted:Boolean(true false)	This is an optional field. Indicates whether Trustsec is trusted. Valid value is true or false.
Trustsec:Notify this device about Trustsec configuration changes:String(ENABLE_ALL DISABLE_ALL)	This is an optional field. Notifies Trustsec configuration changes to the Trustsec device. Valid value is ENABLE_ALL or DISABLE_ALL

Field	Description
Trustsec:Include this device when deploying Security Group Tag Mapping Updates:Boolean(true false)	This is an optional field. It is the Trustsec device included on SGT. Valid value is true or false.
Deployment:Execution Mode Username:String(32)	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.
Deployment:Execution Mode Password:String(32)	This is an optional field. It is the device password and is a string, with a maximum of 32 characters in length.
Deployment:Enable Mode Password:String(32)	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.
Trustsec:PAC issue date:Date	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.
Trustsec:PAC expiration date:Date	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.
Trustsec:PAC issued by:String	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.

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 11: CSV Template Fields and Description for Network Device Groups

Field	Description
Name:String(100):	(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 > 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.
Description:String(1024)	This is an optional network device group description. It is a string, with a maximum of 1024 characters in length.

Field	Description
Type:String(64):	(Required) This field is the network device group type. It is a string, with a maximum of 64 characters in length.
Is Root:Boolean(true false):	(Required) This is a field that determines if the specific network device group is a root group. Valid value is true or false.

Mobile Device Manager Interoperability with Cisco ISE

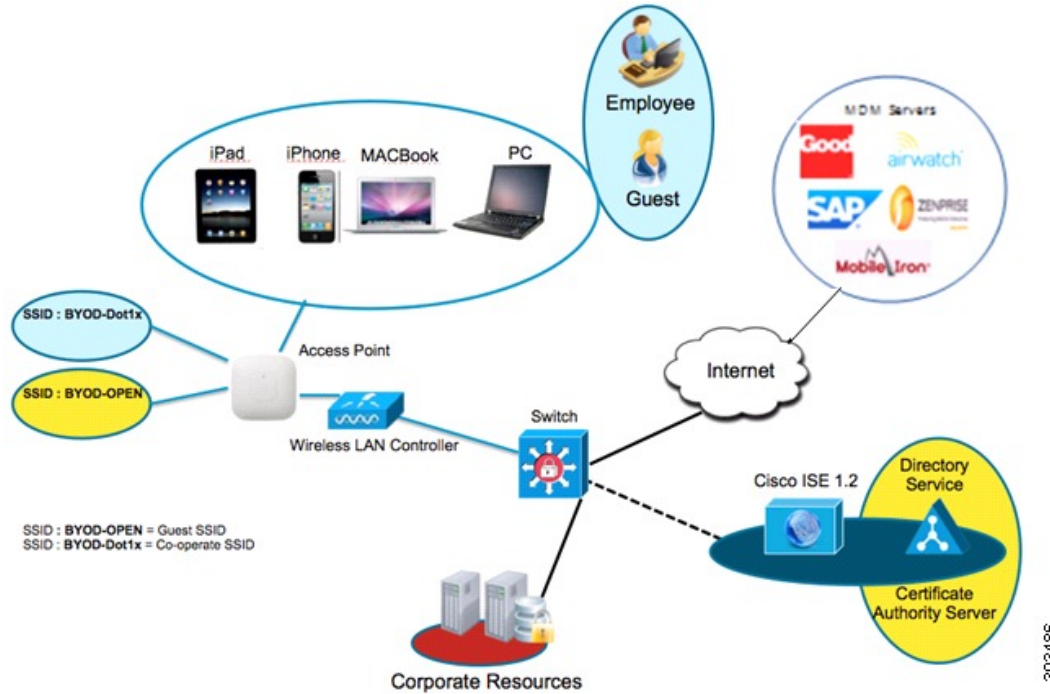
Mobile Device Management (MDM) servers secure, monitor, manage, and support mobile devices deployed across mobile operators, service providers, and enterprises. MDM servers act as a policy server that controls the use of some applications on a mobile device (for example, an e-mail application) in the 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 MDM API 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.

Figure 20: MDM Interoperability with Cisco ISE



The following table lists the components that are used in the MDM setup.

Table 12: Components Used in the MDM Setup

Component	Specification
Cisco Identity Services Engine, Release 1.3 Cisco Identity Services Engine, Release 1.4	Any of the following: ISE 3315, 3355, 3395, 3415, 3495, or VMware
MDM Server	—
(Optional) Certificate Authority Server	As per Microsoft specification (Windows 2008 R2 Enterprise SP2, Windows 2012 R2)
Wireless LAN Controller (WLC)	<ul style="list-style-type: none"> Hardware: 5500 Series, 2500 Series, WLSM-2 Software: Unified Wireless Network Software, Release 7.2, WLC 8.1
Mobile Devices	Devices supported by the MDM vendor. For example, Apple iOS 5.0 and higher, Google Android 3.x and higher.

You can configure Cisco ISE to interoperate with an external Mobile Device Manager (MDM) server. 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 over HTTPS to pull the various pieces of 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.

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 198.

Supported MDM Use Cases

The functions Cisco ISE performs in conjunction with the external MDM server are as follows:

- Facilitating device registration—Unregistered endpoints accessing the network are redirected to a registration page hosted on the MDM server for registration based on user role, device type, and so on.
- Handling device remediation—Endpoints are granted only restricted access.
- 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 **Administration > Identity Management > Identities > Endpoints** page if an endpoint is a MDM monitored device. For example:
 - MDMMimei: 99 000100 160803 3
 - MDMMManufacturer: Apple
 - MDMMModel: iPhone
 - MDMMOSVersion: iOS 6.0.0
 - MDMPhoneNumber: 9783148806
 - MDMSerialNumber: DNPGQZGUDTF9
- Cisco ISE polls the MDM server once every four 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.

Cisco ISE allows you to configure MDM policy based on the following attributes:

- DeviceRegisterStatus
- DeviceCompliantStatus
- DiskEncryptionStatus
- PinLockStatus

- JailBrokenStatus
- Manufacturer
- IMEI
- SerialNumber
- OsVersion
- PhoneNumber
- MDMServerName
- MDMServerReachable
- MEID
- Model
- UDID

Supported MDM Servers

Supported MDM servers include products from the following vendors:

- Airwatch, Inc.
- Good Technology
- MobileIron, Inc.
- Zenprise, Inc.
- SAP Afaria
- Fiberlink MaaS
- Meraki

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 13: Ports Used by the MDM Server

MDM Server	Ports
Mobile Iron	443
Zenprise	443
Good	19005
Airwatch	443

MDM Server	Ports
Afaria	443
Fiberlink MaaS	443
Meraki	443
Microsoft Intune	80 and 443
Microsoft SCCM	80 and 443

MDM Dictionary Attributes

After you add the MDM server definition in Cisco ISE, the MDM dictionary attributes are available in Cisco ISE that you can use in authorization policies. You can view the dictionary attributes that are available for use in authorization policies.

When you are using these MDM dictionary attributes in policies, you cannot delete the MDM server configuration from Cisco ISE. To remove the MDM server configuration, you must first remove the MDM dictionary attributes from policies, and then remove the MDM server from Cisco ISE.

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.

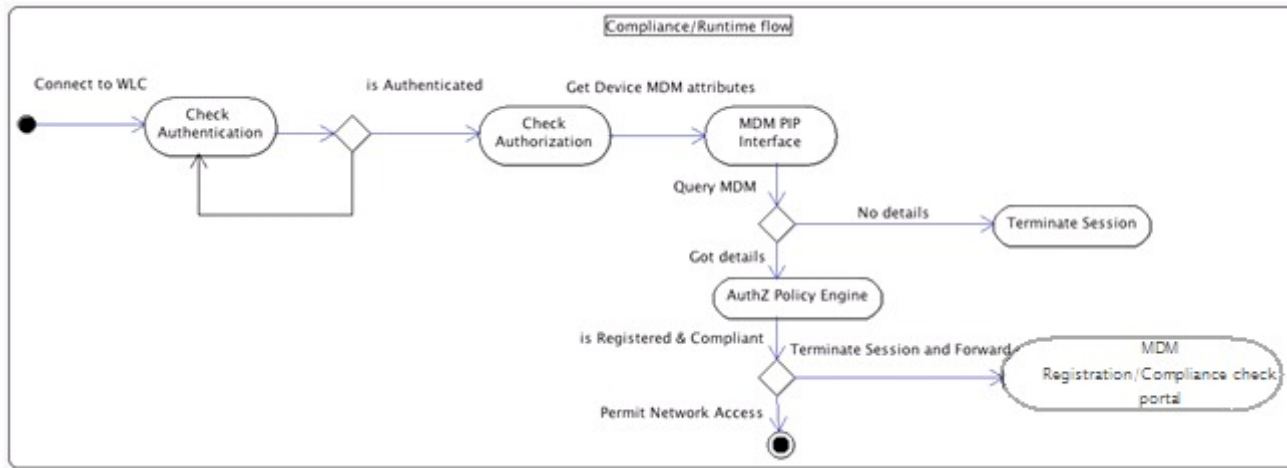


Note A device that was enrolled on the MDM server outside of a Cisco ISE network will be automatically registered with Cisco ISE if it is compliant with the posture policies.

- 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.



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.
 - Step 2** Create mobile device manager definitions.
 - Step 3** Configure ACLs on the Wireless LAN Controllers.
 - Step 4** Configure authorization profile for redirecting non-registered devices.
 - Step 5** If there are 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.

-
- 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.
-

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 52](#)
- [Set Permissions for Access to WMI Root/CIMv2 Name Space, on page 54](#)
- [Grant Access to the Security Event Log on the AD Domain Controller, on page 55](#)

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

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 ID Mapping 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 21: Local and Remote Access for Access Permissions

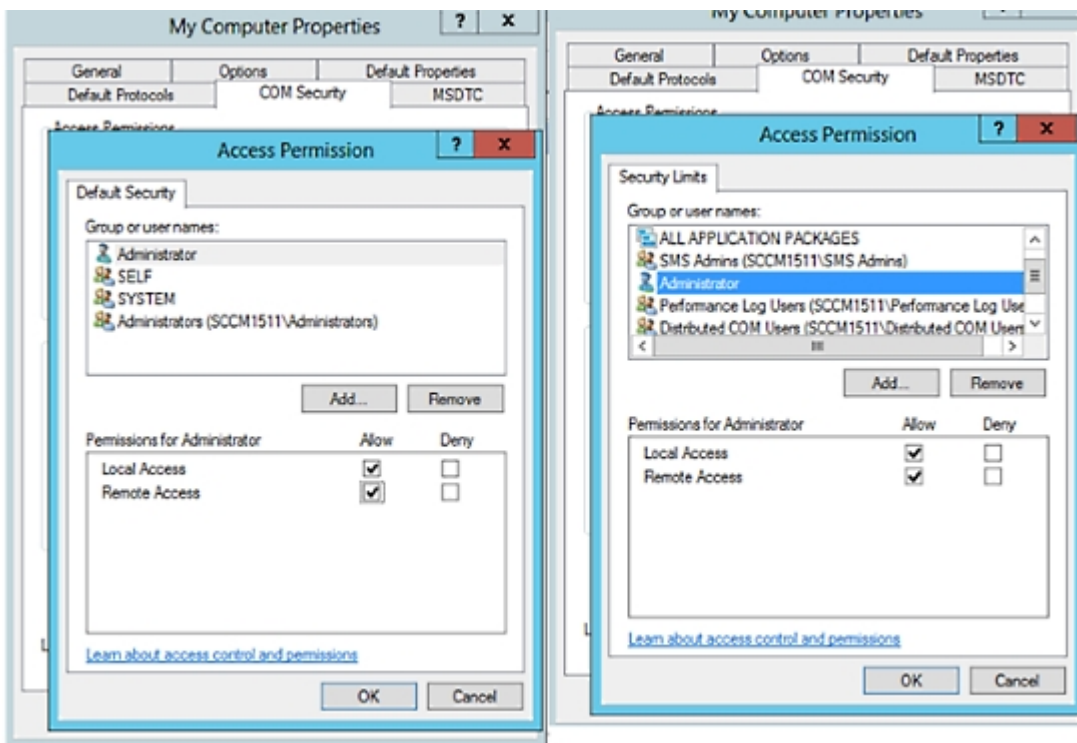
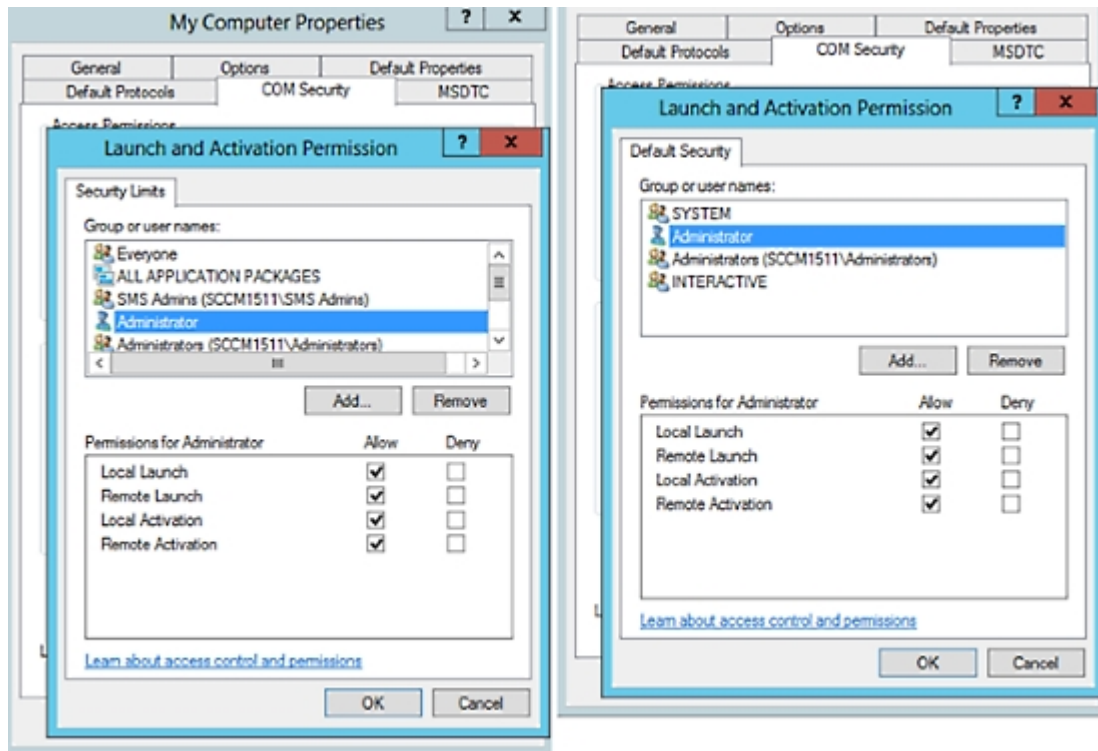


Figure 22: Local and Remote Access for Launch and Activation Permissions

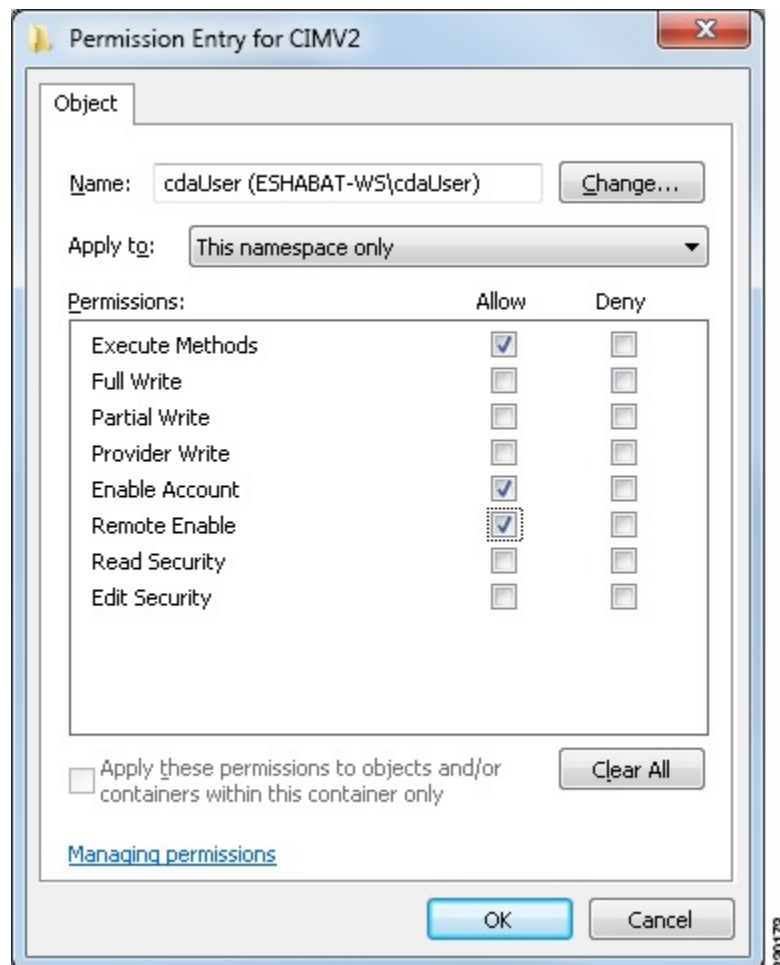


Set Permissions for Access to WMI Root/CIMv2 Name Space

By default, Active Directory users do not have permissions for the Execute Methods and Remote Enable. You can grant access using the `wmicmgmt.msc` MMC console.

- Step 1** Click Start > Run and type `wmicmgmt.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.

Figure 23: Required Permissions for WMI Root\CIMv2 Name Space



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

Higher ports are assigned dynamically or you can configure them manually. We recommend that you add %SystemRoot%\System32\dlhhost.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.

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 gets 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.](#)

Related Topics

[Configure Authorization Policy Rules for the MDM Use Cases, on page 208](#)

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.

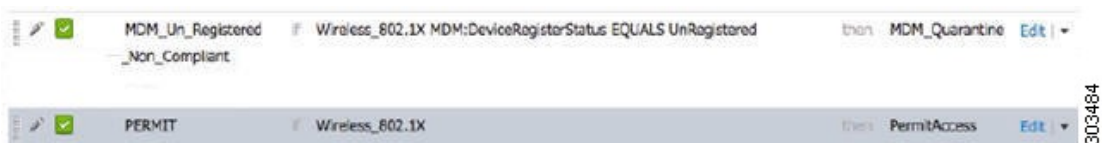
Step 1 Choose **Policy > Authorization > Insert New Rule Below**.

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 24: Authorization Policy Rules for the MDM Use Cases



Step 3 Click **Save**.

Related Topics

[Import MDM Server Certificate into Cisco ISE, on page 201](#)

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 **Administration > Identity Management > 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.

Related Topics

- [Mobile Device Manager Interoperability with Cisco ISE, on page 195](#)
- [Supported MDM Use Cases, on page 197](#)
- [View Mobile Device Manager Logs, on page 209](#)
- [Supported MDM Servers, on page 198](#)

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."

Related Topics

- [Mobile Device Manager Interoperability with Cisco ISE, on page 195](#)
- [Supported MDM Use Cases, on page 197](#)
- [View Mobile Device Manager Reports, on page 209](#)
- [Supported MDM Servers, on page 198](#)



Manage Resources

- [Dictionaries and Dictionary Attributes, page 211](#)
- [RADIUS-Vendor Dictionaries, page 213](#)

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, 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.
- Add or remove allowed values for dictionary attributes.

Create User-Defined Dictionaries

You can create, edit, or delete user-defined dictionaries.

-
- Step 1** Choose **Policy > Policy Elements > Dictionaries > User**.
- Step 2** Click **Add**.
- Step 3** Enter the name for the user dictionary, an optional description, and a version for the user dictionary.
- Step 4** Choose the attribute type from the Dictionary Attribute Type drop-down list.
- Step 5** Click **Submit**.
-

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.

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**.
-

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**.
-



Logging Mechanism

- [Cisco ISE Logging Mechanism, page 215](#)
- [Cisco ISE System Logs, page 216](#)
- [Configure Remote Syslog Collection Locations, page 221](#)
- [Cisco ISE Message Codes, page 222](#)
- [Cisco ISE Message Catalogs, page 222](#)
- [Debug Logs, page 222](#)
- [Endpoint Debug Log Collector, page 223](#)
- [Collection Filters, page 224](#)

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.



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.

Local Store Syslog Message Format

Log messages are sent to the local store with this syslog message format:

timestamp sequence_num msg_ode msg_sev msg_class msg_text attr =value

Field	Description
<i>timestamp</i>	<p>Date of the message generation, according to the local clock of the originating the Cisco ISE node, in the following format : <i>YYYY-MM-DD hh:mm:ss:xxx +/-zh:zm</i>. Possible values are:</p> <ul style="list-style-type: none"> • <i>YYYY</i> = Numeric representation of the year. • <i>MM</i> = Numeric representation of the month. For single-digit months (1 to 9) a zero precedes the number. • <i>DD</i> = Numeric representation of the day of the month. For single-digit days (1 to 9), a zero precedes the number. • <i>hh</i> = The hour of the day—00 to 23. • <i>mm</i> = The minute of the hour—00 to 59. • <i>ss</i> = The second of the minute—00 to 59. • <i>xxx</i> = The millisecond of the second—000 to 999. • <i>+/-zh:zm</i> = The time zone offset from the Cisco ISE server's time zone, where <i>zh</i> is the number of offset hours and <i>zm</i> 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, <i>+02:00</i> 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.
<i>sequence_num</i>	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 999999999.
<i>msg_ode</i>	Message code as defined in the logging categories.

Field	Description
<i>msg_sev</i>	Message severity level of a log message. See Administration > System > Logging > Logging Categories .
<i>msg_class</i>	Message class, which identifies groups of messages with the same context.
<i>msg_text</i>	English language descriptive text message.
<i>attr=value</i>	<p>Set of attribute-value pairs that provides details about the logged event. A comma (,) separates each pair.</p> <p>Attribute names are as defined in the Cisco ISE dictionaries.</p> <p>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.</p> <p>For example, Response={RadiusPacketType=AccessAccept; AuthenticationResult=UnknownUser; cisco-av-pair=sga:security-group-tag=0000-00;}</p>

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 YYYY Mmm DD hh:mm:ss xx:xx:xx:xx/host_name cat_name msg_id total_seg seg_num
```


Field	Description
<i>pri_num</i>	<p>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.</p> <p>The facility code valid options are:</p> <ul style="list-style-type: none">• 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)

Field	Description
<i>time</i>	<p>Date of the message generation, according to the local clock of the originating Cisco ISE server, in the format YYYY Mmm DD hh:mm:ss.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • YYYY = Numeric representation of the year. • Mmm = Representation of the month—Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • 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. <p>Some device 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.</p>
<i>xx:xx:xx:xx/host_name</i>	IP address of the originating Cisco ISE node, or the hostname.
<i>cat_name</i>	Logging category name preceded by the CSCOxxx string.

Field	Description
<i>msg_id</i>	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.
<i>total_seg</i>	Total number of segments in a log message. Long messages are divided into more than one segment. Note The <i>total_seg</i> depends on the Maximum Length setting in the remote logging targets page. See <i>Remote Logging Target Settings</i> .
<i>seg_num</i>	Segment sequence number within a message. Use this number to determine what segment of the message you are viewing.

The syslog message data or payload is the same as the [Local Store Syslog Message Format](#). The remote syslog server targets are identified by the facility code names LOCAL0 to LOCAL7 (LOCAL6 is the default logging location.) Log messages that you assign to the remote syslog server are sent to the default location for Linux syslog (/var/log/messages), however; you can configure a different location on the server.

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** Configure the field as necessary.
 - Step 4** Click **Save**.
 - Step 5** Go to the Remote Logging Targets page and verify the creation of the new target. After you have created the syslog storage location on logging target page, you should map the storage location to the required logging categories, to receive the logs.
-

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.

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. The data available in this page are for display only.

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 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.

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.
- 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 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.
-

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**.
-

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.



Backup and Restore Operations

- [Backup Data Type, page 227](#)
- [Backup and Restore Repositories, page 228](#)
- [On-Demand and Scheduled Backups, page 229](#)
- [Cisco ISE Restore Operation, page 234](#)
- [Export Authentication and Authorization Policy Configuration, page 240](#)
- [Synchronize Primary and Secondary Nodes in a Distributed Environment, page 240](#)
- [Recovery of Lost Nodes in Standalone and Distributed Deployments, page 240](#)

Backup Data Type

Cisco ISE allows you to back up data from the primary or standalone Administration node and from the Monitoring node. Backup can be done from the CLI or user interface.

When Cisco ISE is run on VMware, VMware snapshots are not supported for backing up ISE data.

VMware snapshot saves the status of a VM at a given point of 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.

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.
- **Operational Data**—Contains monitoring and troubleshooting data.

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 1.21.3, you can restore it on Cisco ISE, Release 1.31.4.

Cisco ISE, Release 1.4 supports restore from backups obtained from Release 1.2 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

For the SNS 3415 and SNS 3495 Appliances, there is no physical CD-ROM available. You can create the repository type as CD-ROM for the virtual CD-ROM created using the KVM.

**Note**

Repositories are local to each device.

**Note**

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.

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 Administration Node (PAN) get replicated to the other deployment nodes.

Before You Begin

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

-
- 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 702](#) 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.

On-Demand and Scheduled Backups

Cisco ISE provides on-demand backups of the 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.

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 Click **Backup Now**.

Step 3 Enter the values as required to perform a backup.

Step 4 Click **OK**.

Step 5 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.

Schedule a Backup

You can use this page to schedule configuration or monitoring backups.

**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 types of data that can be backed up and on-demand and scheduled backups.
- 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 **Create** 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** Click the **Refresh** link at the top of this page 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.
-

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 reimaged 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 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 PAN, you must manually synchronize the secondary nodes with the 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.

Guidelines for Data Restoration

Following are guidelines to follow when you restore Cisco ISE backup data.

- If you obtain a backup from the 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 PAN with a different hostname than the one from which the backup was obtained, the 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 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 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 PAN, generate the root CA and subordinate CAs on the PAN and Policy Service Nodes (PSNs).

- 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 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 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 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.
<i>filename</i>	Name of the backed-up file that resides in the repository. Supports up to 120 alphanumeric characters. Note You must add the .tar.gpg extension after the filename (for example, myfile.tar.gpg).
repository	Specifies the repository that contains the backup.
<i>repository-name</i>	Name of the repository you want to restore the backup from.
encryption-key	(Optional) Specifies user-defined encryption key to restore backup.
hash	Hashed encryption key for restoring backup. Specifies an encrypted (hashed) encryption key that follows. Supports up to 40 characters.
plain	Plaintext encryption key for restoring backup. Specifies an unencrypted plaintext encryption key that follows. Supports up to 15 characters.
<i>encryption-key name</i>	Enter the encryption key.

include-adeos	(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.
----------------------	--

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 Alert Process...
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

	Description
backup	Performs a backup (Cisco ISE and Cisco ADE OS) and places the backup in a repository.
backup-logs	Backs up system logs.
repository	Enters the repository submode for configuration of backups.
show repository	Displays the available backup files located on a specific repository.

	Description
show backup history	Displays the backup history of the system.
show backup status	Displays the status of the backup operation.
show restore status	Displays the status of the restore operation.

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 PAN and perform a manual synchronization.

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 Administration Node (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 Administration Node 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 PAN and restore it on the secondary Administration node. This ensures that the secondary Administration node can function as the root CA or subordinate CA of an external PKI in case of a PAN failure and you promote the secondary Administration node to be the PAN.

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.

Restore a Monitoring 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.

-
- Step 1** Choose **Administration** > **System** > **Backup and Restore**.
- Step 2** Select the name of the backup from the list of Operational backup and click **Restore**.
- Step 3** Enter the Encryption Key used during the backup.
- Step 4** Click **Restore**.
-

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** Prepare to promote another Cisco ISE node as the PAN, by synchronizing the node with the existing primary node you want to backup.
This ensures that the configuration of the Cisco ISE node you are going to promote is up to date.
- Step 2** Promote the newly synced Administration node to primary status.
- Step 3** Prepare to deregister the node to be backed up by assigning the Monitoring persona to another node in the deployment. A deployment must have at least one functioning Monitoring node.

- Step 4** Deregister the node to be backed up.
 - Step 5** Restore the Monitoring backup to the newly deregistered node.
 - Step 6** Register the newly restored node with the current Administration node.
 - Step 7** Promote the newly restored and registered node as the PAN.
-

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.
-

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.

-
- Step 1** Choose **Administration** > **System** > **Backup & Restore**.
 - Step 2** Click **Policy Export**.
 - Step 3** Enter the values as needed.
 - Step 4** Click **Export**.
Use a text editor such as WordPad to view the contents of the XML file.
-

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 check boxes 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 Administration Node or PAN) and N2 (Secondary Administration 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.

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.

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 Administration Node or 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 (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.

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.

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.

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 Administration Node or PAN) and N2 (Secondary Administration Node) 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.

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 (PAN), N2 (Secondary Administration Node), 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 Endpoint Protection Service Adaptive Network Control

- [Enable Endpoint Protection Service Adaptive Network Control in Cisco ISE](#), page 245
- [Configure Network Access Settings](#), page 245
- [Endpoint Protection Service Adaptive Network Control](#), page 247
- [EPSANC Quarantine and Unquarantine Flow](#), page 249
- [EPSANC NAS Port Shutdown Flow](#), page 250
- [Endpoints Purge Settings](#), page 250

Enable Endpoint Protection Service Adaptive Network Control in Cisco ISE

Endpoint Protection Service (EPS) Adaptive Network Control (ANC) is disabled by default. You must enable EPS ANC manually, and it remains enabled until you manually disable the service in the Admin portal.

You must have Super Admin and Policy Admin role privileges to enable EPS ANC in Cisco ISE.

-
- Step 1** Choose **Administration > System > Settings > Endpoint Protection Service > Adaptive Network Control**.
 - Step 2** Click the Service Status drop-down list, and choose **Enabled**.
 - Step 3** Click **Save**.
-

Configure Network Access Settings

Endpoint Protection Service (EPS) 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 EPS ANC to close the NAS port.

Before You Begin

- You must enable EPSANC.
- You must create authorization profiles and Exception type authorization policies for EPSANC.

Step 1 Choose **Operations > Endpoint Protection Service > Adaptive Network Control**.

Step 2 Under **Endpoint Operation**, enter the IP Address or MAC Address of an endpoint.

Step 3 Click the Operations drop-down list to choose one of the following actions:

- **Quarantine**—Isolates the endpoint, restricting access on the network
- **Unquarantine**—Reverses the quarantine process, allowing full access to the network
- **Shutdown**—Closes the NAS port to which the endpoint is connected

Step 4 Click **Submit**.

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.

**Note**

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.

Endpoint Protection Service Adaptive Network Control

Endpoint Protection Service (EPS) 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. EPS is also known as Adaptive Network Control (ANC). EPS ANC can be invoked by the ISE administrator on the admin GUI and also through pxGrid from third party systems. EPS ANC supports wired and wireless deployments and requires a Plus License.

You can use EPS ANC to change the authorization state without having to modify the overall authorization policy of the system. EPS 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 EPS 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.

**Note**

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.

Create Authorization Profiles for Network Access through EPSANC

You must create an authorization profile for use with EPS 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 1** Choose **Policy > Policy Elements > Authorization > Authorization Profiles**.
 - 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**.
-

Create Exception Policies for Network Access through EPSANC

For EPS ANC authorization, you must create a quarantine exception policy that is processed before all standard authorization policies. Exception authorization policies are intended for authorizing limited access to meet special conditions or permissions or an immediate requirement. Standard authorization policies are intended to be stable and apply to a large groups of users, devices, and groups that share a common set of privileges.

Before You Begin

You should have successfully created standard authorization profiles for use with EPS ANC.

-
- Step 1** Choose **Policy > Authorization**, and expand **Exceptions**.
 - Step 2** Choose **Enabled** or **Disabled** or **Monitor Only** option.
 - Step 3** Click **Create a New Rule**.
 - Step 4** Enter the exception rule name.
 - Step 5** Click the plus [+] sign to choose an identity group.
 - Step 6** Click the plus [+] sign to choose **Create New Condition (Advanced Option)**.
 - Step 7** Click the down arrow icon in the first field to display the dictionaries list and choose **Session > EPSStatus**.
 - Step 8** Choose **Equals** from the drop-down list in the second field.
 - Step 9** Choose **Quarantine** from the drop-down list in the third field.
 - Step 10** Click **Save**.
-

EPSANC Operations Fail when IP Address or MAC Address is not Found

An EPS 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 EPS 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, IP Address or Session ID.

Externally Authenticated Administrators Cannot Perform EPSANC 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 EPS ANC operation from Operations > Endpoint Protection Service 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:

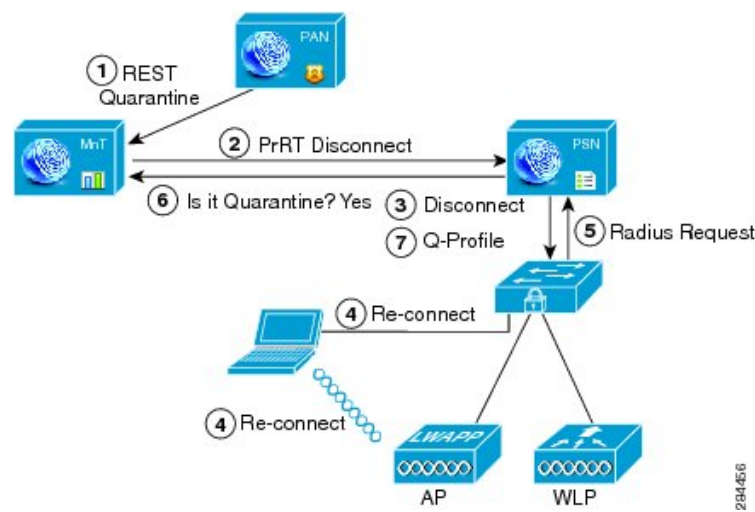
Server failure: User not found internally. Possible use of unsupported externally authenticated user

EPSANC Quarantine and Unquarantine Flow

You can quarantine selected endpoints with EPS 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 EPS ANC session has been established.

Figure 25: EPS 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.

EPSANC 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 shut down command, however. You can use the getResult() command to verify that the shutdown executed successfully.

This figure illustrates the EPS 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 26: EPS 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 Administration Node (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, page 255](#)
- [Configure Guest Access, page 319](#)
- [Support Device Access, page 365](#)
- [Customize End-User Web Portals, page 385](#)



Manage Users and External Identity Sources

- [Cisco ISE Users, page 255](#)
- [Internal and External Identity Sources, page 260](#)
- [Certificate Authentication Profiles, page 262](#)
- [Active Directory as an External Identity Source, page 263](#)
- [ISE pxGrid Identity Mapping, page 282](#)
- [LDAP, page 295](#)
- [RADIUS Token Identity Sources, page 303](#)
- [RSA Identity Sources, page 307](#)
- [SAMLv2 Identity Provider as an External Identity Source, page 312](#)
- [Identity Source Sequences, page 316](#)
- [Identity Source Details in Reports, page 317](#)

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

On the User Custom Attributes Setting page, you can use the Custom Attributes pane to define additional user-account attributes. Cisco ISE provides a list of predefined attributes that are not configurable. However, you can define custom attributes by configuring the following:

- Attribute name
- Data type

User Password Policy Settings

You can define the criteria that user-account passwords must meet in the User Password Policy page. Choose **Administration > Identity Management > Settings > User Password Policy**.

The following table describes the fields in the User Password Policy page.

Table 14: User Password Policy Settings

Setting	Description
Minimum length	Sets the minimum length of the password (in characters)
Username	Restricts the use of the username or its characters in reverse order
Cisco	Restricts the use of "cisco" or its characters in reverse order
Special characters	Restricts the use of special characters that you define in reverse order
Repeated characters	Restricts the use of characters repeated four or more times consecutively
Required characters	<p>Requires that the password include at least one of each of the following types:</p> <ul style="list-style-type: none"> • Lowercase alphabetic characters • Uppercase alphabetic characters • Numeric characters • Non-alphanumeric characters <p>If a user-password policy requires upper or lowercase characters and 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, you must uncheck the following check box options:</p> <ul style="list-style-type: none"> • Lowercase alphabetic characters • Uppercase alphabetic characters
Password History	Specifies the number of previous versions from which the password must be different to prevent repeated use of the same password

Setting	Description
Password Lifetime	<p>Sets the following options to force users to change passwords after a specified time period:</p> <ul style="list-style-type: none"> • Time (in days) before the user account is disabled if the password is not changed • Reminder (in days) before the user account is disabled

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**.
- 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 User Data

Instead of entering user accounts manually into Cisco ISE, you can import them. Cisco ISE allows you to import user data in the form of a csv file into its internal database.

-
- 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 this type of file.
 - 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** check boxes 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**.
 - Step 2** Enter values in the Name and Description fields. Supported characters for the Name field are space # \$ & ' () * + - . / @ _ .
 - Step 3** Click **Submit**.
-

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.
-

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.

Table 15: Authentication Protocols and Supported External Identity Sources

Protocol (Authentication Type)	Internal Database	Active Directory	LDAP	RADIUS Token Server or RSA
EAP-GTC, PAP (plain text password)	Yes	Yes	Yes	Yes

Protocol (Authentication Type)	Internal Database	Active Directory	LDAP	RADIUS Token Server or RSA
MS-CHAP password hash: MSCHAPv1/v2 EAP-MSCHAPv2 (as inner method of PEAP or EAP-FAST) LEAP	Yes	Yes	No	No
EAP-MD5 CHAP	Yes	No	No	No
EAP-TLS PEAP-TLS (certificate retrieval) Note For TLS authentications (EAP-TLS and PEAP-TLS), identity sources are not required but can optionally be added for authorization policy conditions.	No	Yes	Yes	No

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 includes certificate authentication profiles that you need for certificate-based authentications.

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 263 for more details).
- **LDAP** to add an LDAP identity source (see [LDAP](#), on page 295 for more details).
- **RADIUS Token** to add a RADIUS Token server (see [RADIUS Token Identity Sources](#), on page 303 for more details).
- **RSA SecurID** to add an RSA SecurID server (see [RSA Identity Sources](#), on page 307 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 312 for more details).

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.

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 16: Authentication Protocols Supported by Active Directory

Authentication Protocols	Features
EAP-FAST and password based Protected Extensible Authentication Protocol (PEAP)	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
Password Authentication Protocol (PAP)	User and machine authentication
Microsoft Challenge Handshake Authentication Protocol Version 1 (MS-CHAPv1)	User and machine authentication
Microsoft Challenge Handshake Authentication Protocol Version 2 (MS-CHAPv2)	User and machine authentication
Extensible Authentication Protocol-Generic Token Card (EAP-GTC)	User and machine authentication
Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)	<ul style="list-style-type: none"> • User and machine authentication • Groups and attributes retrieval • Binary certificate comparison
Extensible Authentication Protocol- Flexible Authentication via Secure Tunneling-Transport Layer Security (EAP-FAST-TLS)	<ul style="list-style-type: none"> • User and machine authentication • Groups and attributes retrieval • Binary certificate comparison
Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)	<ul style="list-style-type: none"> • User and machine authentication • Groups and attributes retrieval • Binary certificate comparison

Authentication Protocols	Features
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.

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

See Microsoft-imposed limits on the maximum number of usable Active Directory groups:
[http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability\(v=WS.10\).aspx](http://technet.microsoft.com/en-us/library/active-directory-maximum-limits-scalability(v=WS.10).aspx)

An authorization policy fails if the rule contains an Active Directory group name with special characters such as /, !, @, \, #, \$, %, ^, &, *, (,), _, +, or ~.

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.

Additionally, you can set the IdentityAccessRestricted attribute if conditions mentioned above (for example, user disabled) are met. IdentityAccessRestricted attribute is set in order to support legacy policies and is not required in Cisco ISE 1.31.4 because authentication fails if such conditions (for example, user disabled) are 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

The following are the prerequisites to integrate Active Directory with Cisco 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.
- If your Active Directory structure has multidomain forest or is divided into multiple forests, ensure that trust relationships exist between the domain to which Cisco ISE is connected and the other domains that have user and machine information to which you need access. 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

Join Operations	Leave Operations	Cisco ISE Machine Accounts
<p>For the account that is used to perform the join operation, the following permissions are required:</p> <ul style="list-style-type: none"> • Search Active Directory (to see if a Cisco ISE machine account already exists) • Create Cisco ISE machine account to domain (if the machine account does not already exist) • Set attributes on the new machine account (for example, Cisco ISE machine account password, SPN, dnsHostname) <p>It is not mandatory to be a domain administrator to perform a join operation.</p>	<p>For the account that is used to perform the leave operation, the following permissions are required:</p> <ul style="list-style-type: none"> • Search Active Directory (to see if a Cisco ISE machine account already exists) • Remove Cisco ISE machine account from domain <p>If you perform a force leave (leave without the password), it will not remove the machine account from the domain.</p>	<p>For the newly created Cisco ISE machine account that is used to communicate to the Active Directory connection, the following permissions are required:</p> <ul style="list-style-type: none"> • Ability to change own password • Read the user/machine objects corresponding to users/machines being authenticated • Query some parts of the Active Directory to learn about required information (for example, trusted domains, alternative UPN suffixes and so on.) • Ability to read tokenGroups attribute <p>You can precreate the machine account in Active Directory, and if the SAM name matches the Cisco ISE appliance hostname, it should be located during the join operation and re-used.</p> <p>If multiple join operations are performed, multiple machine accounts are maintained inside Cisco ISE, one for each join.</p>


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.

Network Ports That Must Be Open for Communication

Protocol	Port (remote-local)	Target	Authenticated	Notes
DNS (TCP/UDP)	Random number greater than or equal to 49152	DNS Servers/AD Domain Controllers	No	—
MSRPC	445	Domain Controllers	Yes	—
Kerberos (TCP/UDP)	88	Domain Controllers	Yes (Kerberos)	MS AD/KDC
LDAP (TCP/UDP)	389	Domain Controllers	Yes	—
LDAP (GC)	3268	Global Catalog Servers	Yes	—
NTP	123	NTP Servers/Domain Controllers	No	—
IPC	80	Other ISE Nodes in the Deployment	Yes (Using RBAC credentials)	—

DNS Server

While configuring your DNS server, make sure that you take care of the following:

- All DNS servers configured in Cisco ISE must be able to resolve all forward and reverse DNS queries for all domains you wish to use.
- All DNS server must be able to answer SRV queries for DCs, GCs, and KDCs with or without additional Site information.
- We recommend that you add the server IP addresses to SRV responses to improve performance.
- Avoid using DNS servers that query the public Internet. They can cause delays and leak information about your network when an unknown name has to be resolved

Configure Active Directory as an External Identity Source

Before you configure Active Directory as an External Identity Source, make sure that:

- Cisco ISE hostnames are 15 characters or less in length. Active Directory does not allow hostnames larger than 15 characters.
- 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.



Note If you see operational issues when Cisco ISE is connected to Active Directory, see the AD Connector 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 268
- 2 [Configure Authentication Domains](#), on page 270
- 3 [Configure Active Directory User Groups](#), on page 271
- 4 [Configure Active Directory User and Machine Attributes](#), on page 272
- 5 (Optional) [Modify Password Changes, Machine Authentications, and Machine Access Restriction Settings](#), on page 272

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.

-
- Step 1** Choose **Administration > Identity Management > External Identity Sources > Active Directory**.
- Step 2** Click **Add** and enter the domain name and identity store name.
- Step 3** Click **Submit**.
A pop-up appears asking if you want to join the newly created join point to the domain. Click **Yes** if you want to join immediately.
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 check box 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 check box 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 username 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.

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 `jd@acme.com`.

Step 7

(Optional) Check the **Specify Organizational Unit** check box.

You should check this check box 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 check box. 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 checks whether any group SIDs are still in the old format. If so, 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 are not advertising 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://technet.microsoft.com/en-us/library/bb727055.aspx>

What to Do Next

Configure authentication domains.

Leave the Active Directory Domain

If you no longer need to authenticate users or machines from an 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 check box next to the Cisco ISE node and click **Leave**.
- Step 3** 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 4** If you do not have the Active Directory credentials, check the **No Credentials Available** check box, and click **OK**. If you check the **Leave domain without credentials** check box, 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 improves 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:
- Choose **Add > Select Groups From Directory** to choose an existing group.
 - 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.

-
- Step 1** Choose **Administration** > **Identity Management** > **External Identity Sources** > **Active Directory**.
- Step 2** Click the **Attributes** tab.
- Step 3** Choose **Add** > **Add Attribute** to manually add a attribute, or choose **Add** > **Select Attributes From Directory** to choose a list of attributes from the directory.
- Step 4** If you choose to add attributes from the directory, enter the name of a user in the **Sample User or Machine Account** field, and click **Retrieve Attributes** to obtain a list of attributes for users. For example, enter **administrator** to obtain a list of administrator attributes. You can also enter the asterisk (*) wildcard character to filter the results.
- Note** When you enter an example username, ensure that you choose a user from the Active Directory domain to which the Cisco ISE is connected. When you choose an example machine to obtain machine attributes, be sure to prefix the machine name with “host/” or use the SAM\$ format. For example, you might use host/myhost. The example value displayed when you retrieve attributes are provided for illustration only and are not stored.
- Step 5** Check the check boxes next to the attributes from Active Directory that you want to select, and click **OK**.
- Step 6** If you choose to manually add an attribute, enter a name for the new attribute.
- Step 7** Click **Save**.
-

Modify Password Changes, Machine Authentications, and Machine Access Restriction Settings

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** Modify as required, the Password Change, Machine Authentication, and Machine Access Restrictions (MARs) settings. These option are enabled by default.
- Step 4** 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.
-

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

-
- Step 1** Choose **Administration > Identity Management > External Identity Sources > Active Directory**.
 - Step 2** Click **Scope Mode**.
A default scope called Initial_Scope is created, and all the current join points are placed under this scope.
 - Step 3** To create more scopes, click **Add**.
 - Step 4** Enter a name and a description for the new scope.
 - Step 5** Click **Submit**.
-

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 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 applies 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

Test User tool can be used to verify user authentication. 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 check boxes 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.
-

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.

-
- Step 1** Choose **Administration > Identity Management > External Identity Sources > Active Directory**.
- Step 2** Check the check box next to the configured Active Directory.
- Step 3** Check and ensure that the Local Node status is listed as Not Joined.
- Step 4** Click **Delete**.
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.

-
- Step 1** Choose **Administration > Identity Management > External Identity Source > Active Directory**.
 - Step 2** Click **Node View**.
 - Step 3** Select a node from the **ISE Node** 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.
 - Step 4** Click the join point **Name** link to go to that Active Directory join point page and perform other specific actions.
 - Step 5** Click the **Diagnostic Summary** link to go to the **Diagnostic Tools** page to troubleshoot specific issues. The diagnostic tool displays the latest diagnostics results for each join point per node.
-

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.
- Step 3** Click the **Debug Logs** tab.
- Step 4** Scroll down this page to locate the ad_agent.log file. Click this file to download it.
-

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.

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.

Step 1 Open the Group Policy management editor as shown in the following illustration.



Group Policy Objects selection

239641

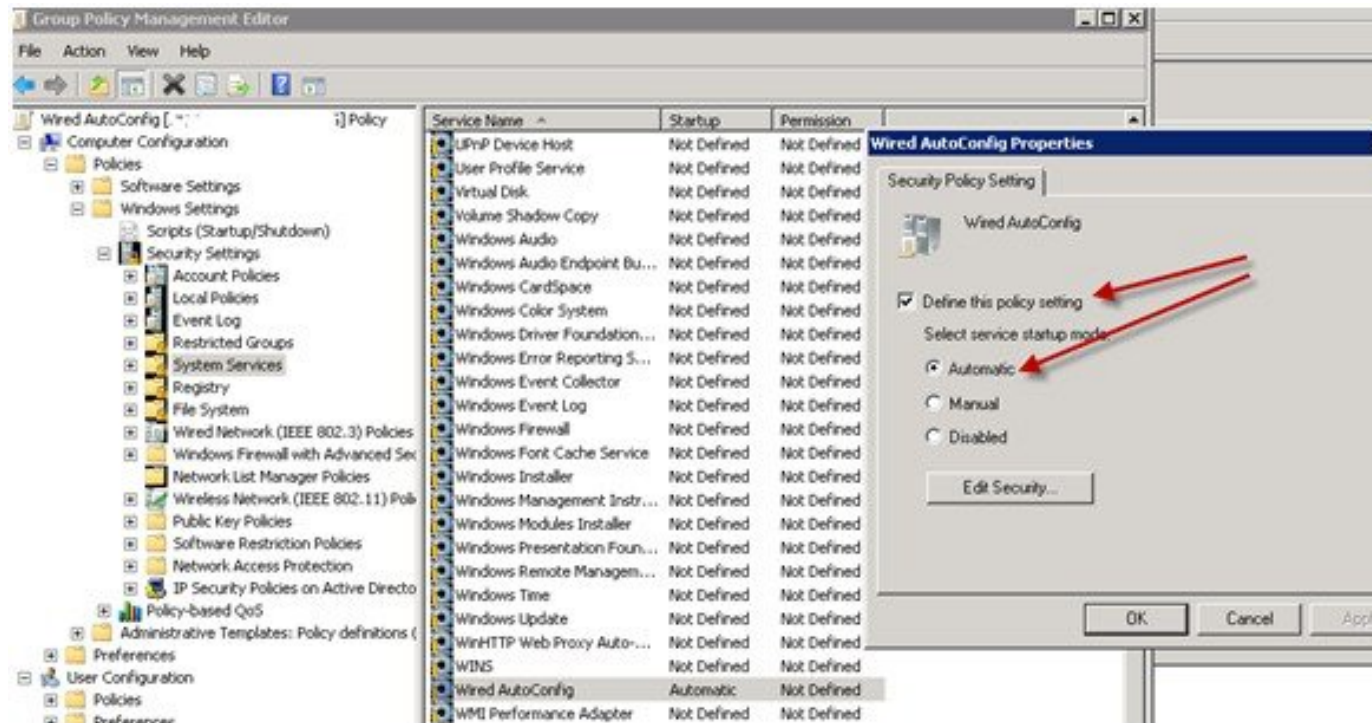
Step 2 Create a new policy and enter a descriptive name for it or add to an existing domain policy.

Example:

In example below, we used Wired Autoconfiguration for the policy name.

- Step 3** Check the **Define this policy setting** check box, and click the **Automatic** radio button for the service startup mode as shown in the following illustration.

Policy Properties



- Step 4** Apply the policy at the desired organizational unit or domain Active Directory level. The computers will receive the policy when they reboot and this service will be turned on.

Configure Odyssey 5.X Suppliant for EAP-TLS Machine Authentications Against Active Directory

If you are using the Odyssey 5.x suppliant for EAP-TLS machine authentications against Active Directory, you must configure the following in the suppliant.

- 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:
- Choose **Configuration > Profiles**.
 - 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.

ISE pxGrid Identity Mapping

Identity Mapping 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, it is possible to use Identity Mapping to collect user authentication information from the active directory (AD) Domain Controller. The Identity Mapping connects to Windows system using the MS WMI interface and queries logs from the Windows event messaging. Once a user logs into the network and is authenticated with an Active Directory, the Domain Controller generates an event log that includes the user name and IP address allocated for the user.

Identity mapping can also be activated even if Cisco ISE plays an active role for authentication. In such cases, the same session may be identified twice. The operational data has a session attribute that indicates the source. You can go to Operations > Authentications and click **Show Live Sessions** to check the Session Source.

The Identity Mapping component retrieves the user logins from the Domain Controller and imports them into the Cisco ISE session directory. So 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, and the AD DC host name and the AD DC NetBios name.

The Cisco ISE plays only a passive role and does not perform the authentication. When Identity Mapping is active, Cisco ISE collects the login information from the AD and includes the data into the session directory.

Key Features

- Identity Mapping is configured from the Cisco ISE administration console. The configuration includes the following settings:
 - Definition of all the DCs from which Identity Mapping is to collect user authentication information. This also includes import and export of the DC list using *.csv files

- DC connection characteristics such as authentication security protocol (NTLMv1 or NTLMv2) and user session aging time
 - Connection testing, to verify the DC is set correctly to initialize valid connection with Identity Mapping
- Identity Mapping report. This report provides information about the Identity Mapping component for troubleshooting
 - Identity Mapping debug logs
 - Cisco ISE session directory maintains the collected user information, so that customers can view it from the Live Sessions and query it from the pxGrid interface
 - Using the CLI command **show application status** provides the health status of nodes that use Identity Mapping
 - Supports High Availability

Configuring Identity Mapping

ID Mapping requires configuration in ISE, and the Active Directory Domain Server must have the right patches and configuration. For information about configuring the Active Directory domain controller for ISE, see [Active Directory Requirements to Support Identity Mapping](#), on page 46

Configure Identity Mapping

ISE must be able to establish a connection with an AD Domain Controller (DC).

Before You Begin

Enable pxGrid services to configure Identity Mapping. Choose **Administration** > **System** > **Deployment** to enable pxGrid services.

To add a new Domain Controller (DC) for Identity Mapping, you need the login credentials of that DC.

Make sure the Domain Controller is properly configured for ISE Identity Mapping, as described in [Active Directory Requirements to Support Identity Mapping](#), on page 46.

-
- Step 1** Choose **Administration** > **pxGrid Identity Mapping** > **AD Domain Controller**.
- Step 2** Click **General Settings**.
- Step 3** The Active Directory General Settings pop-up is displayed. Set the required values and click **Save**.
- **History interval** is the time during which Identity Mapping reads user login information that already occurred. This is required upon startup or restart of Identity Mapping to catch up with events generated while it was unavailable.
 - **User session aging time** is the amount of time the user can be logged in. Identity Mapping 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.
 - You can select either **NTLMv1** or **NTLMv2** as the communications protocol between the ISE and the DC.

- Step 4** Click **Add**.
- Step 5** In the **General Settings** section, enter the **Display Name**, **Domain FQDN**, and **Host FQDN** of the DC.
- Step 6** In the **Credentials** section, enter the Username and Password of the DC.
- Step 7** (Optional) Test the connection to the specified domain by clicking **Verify DC Connection Settings**. This test ensures that the connection to the DC is healthy. However it does not check whether Cisco ISE can fetch the user information upon login.
- Step 8** Click **Submit**. An updated table is displayed with the newly-defined DC included in the list of DCs. The status column indicates the different states of DC.
You can also Import or Export the DC list.
- Note** While importing, you need to provide the password in the template. As the file contains password, the import template should be treated as sensitive. The Export option does not export the password.
-

Filter Identity Mapping

You can filter certain users, based on their name or IP address. 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. The Monitoring live session shows Identity Mapping components that are not filtered out by the Mapping Filters.

-
- Step 1** Choose **Administration > pxGrid Identity Mapping > Mapping Filters**.
- Step 2** Click **Add**, enter the Username and or IP address of the user you want to filter and click **Submit**.
- Step 3** To view the non-filtered users that are currently logged into the Monitoring session directory, choose **Operations > Authentications**.
-

Active Directory Requirements to Support Identity Mapping

Identity Mapping uses 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 logins information. The following sections show how configure the Active Directory domain controller to support ISE Identity Mapping .

Configure Active Directory for Identity Mapping

ISE Identity Mapping uses 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>

This patch fixes a memory leak in Microsoft's WMI, which prevents CDA to establish successful connection with the domain controller (CDA administrator can experience it in CDA Active Directory domain controller GUI page, where the status need to be "up" once the connection establishes successfully).

- <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 CDA 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>

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 CDA may not get all user login events from this domain controller.

- <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>

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:

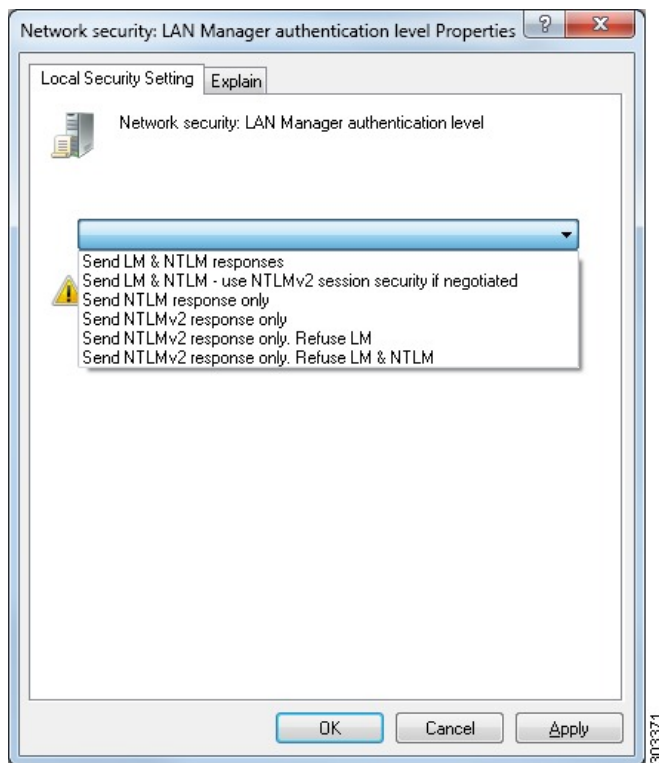
- Permissions Required when an Active Directory User is a Member of the Domain Admin Group, page 2-4
- Permissions Required when an Active Directory User is Not a Member of the Domain Admin Group, page 2-4

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 17: Supported Authentication Types Based on ISE and AD NTLM Version Settings

ISE NTLM setting options / Active Directory (AD) NTLM setting options NTLMv1 NTLMv2	NTLMv1	NTLMv2
Send LM & NTLM responses connection is allowed connection is allowed	connection is allowed	connection is allowed
Send LM & NTLM - use NTLMv2 session security if negotiated connection is allowed connection is allowed	connection is allowed	connection is allowed
Send NTLM response only connection is allowed connection is allowed	connection is allowed	connection is allowed
Send NTLMv2 response only connection is allowed connection is allowed	connection is allowed	connection is allowed
Send NTLMv2 response only. Refuse LM connection is allowed connection is allowed	connection is allowed	connection is allowed
Send NTLMv2 response only. Refuse LM & NTLM connection is refused connection is allowed	connection is refused	connection is allowed

Figure 27: MS NTLM Authentication Type Options**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.
- Step 4** Choose **Default Domain Controllers Policy > Computer Configuration > Policies > Windows Settings > Security Settings**.
- 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 52](#)
- [Set Permissions for Access to WMI Root/CIMv2 Name Space, on page 54](#)
- [Grant Access to the Security Event Log on the AD Domain Controller, on page 55](#)

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

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 ID Mapping 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 28: Local and Remote Access for Access Permissions

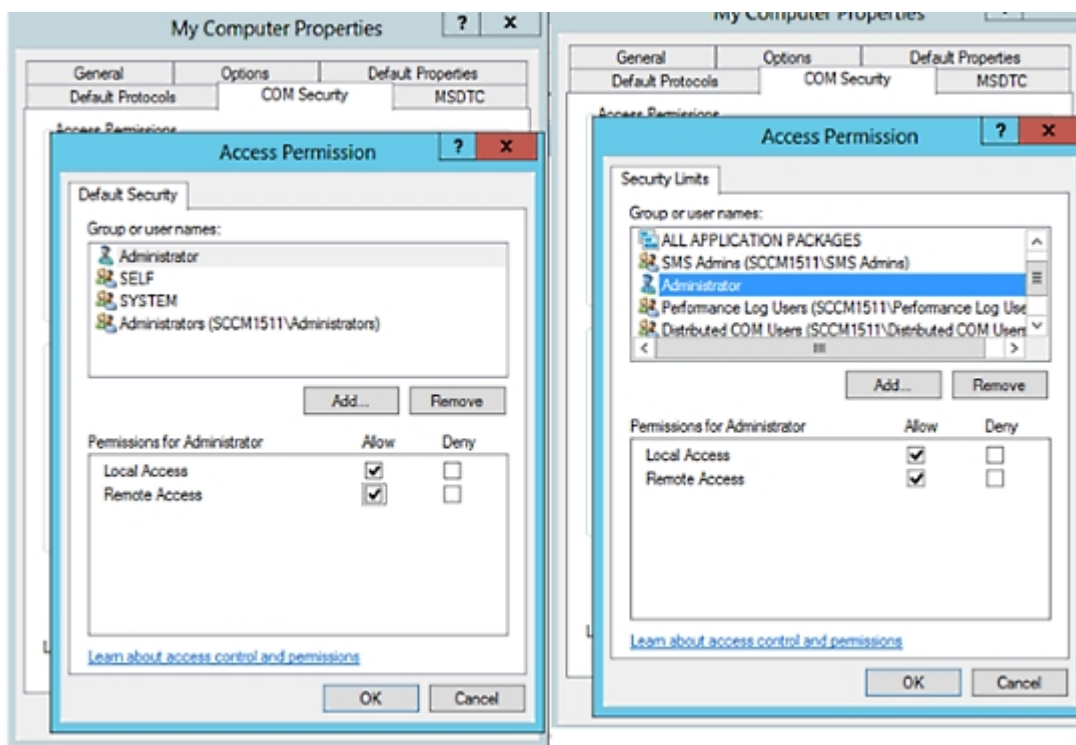
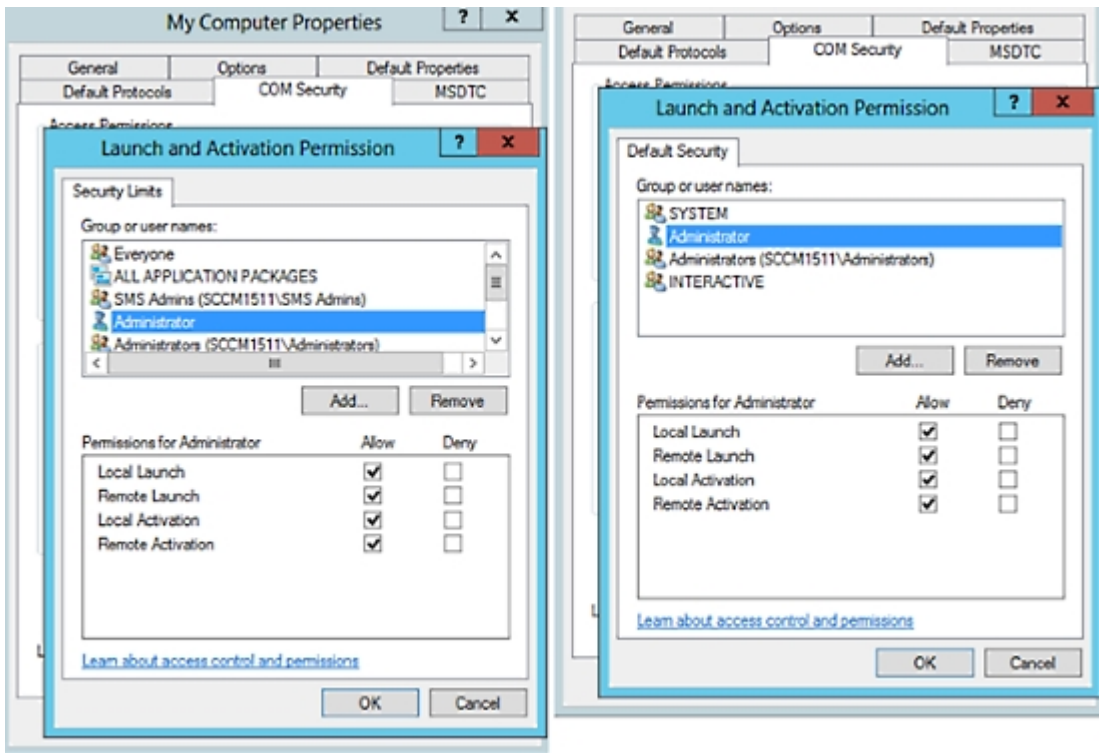


Figure 29: Local and Remote Access for Launch and Activation Permissions

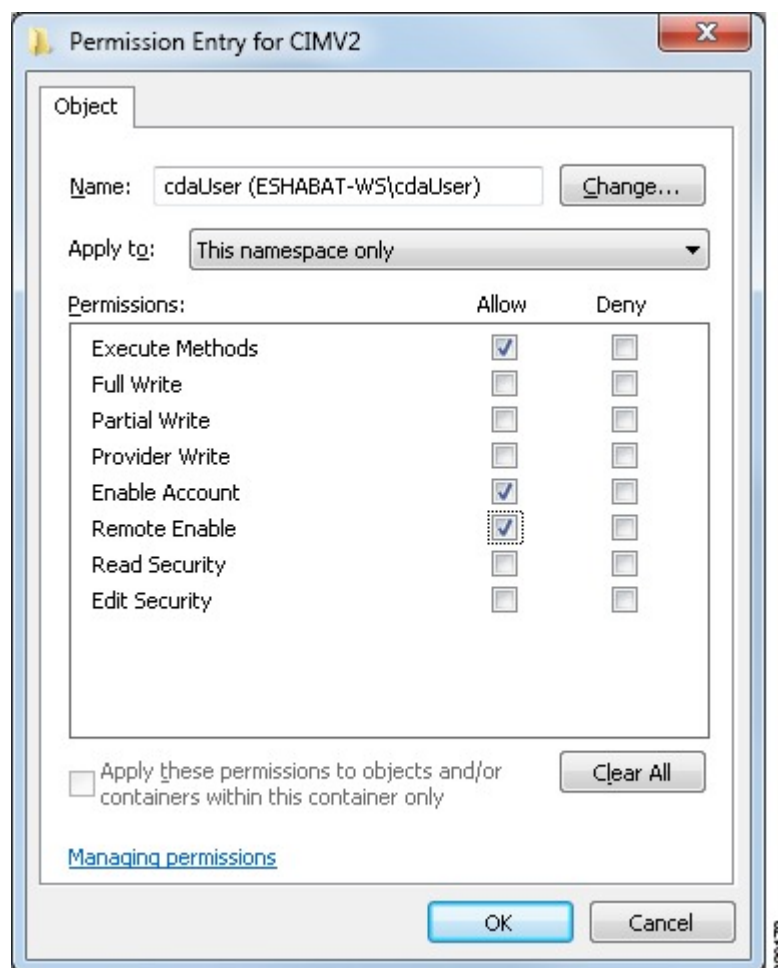


Set Permissions for Access to WMI Root/CIMv2 Name Space

By default, Active Directory users do not have permissions for the Execute Methods and Remote Enable. You can grant access using the `wmimgmt.msc` MMC console.

- Step 1** Click Start > Run and type `wmimgmt.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.

Figure 30: Required Permissions for WMI Root/CIMv2 Name Space



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 .

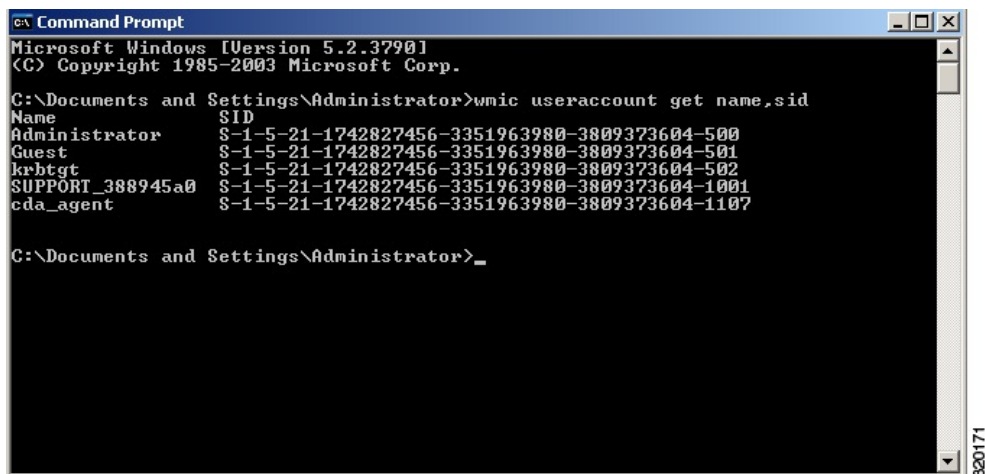
Step 2 Use the following command from the command line, also shown in the diagram below, to list all the SID accounts.

```
wmic useraccount get name,sid
```

You can also use the following command for a specific username and domain:

```
wmic useraccount where name="cdaUser" get domain,name,sid
```

Figure 31: List All the SID Accounts



```

C:\Documents and Settings\Administrator>wmic useraccount get name,sid
Name                SID
Administrator      S-1-5-21-1742827456-3351963980-3809373604-500
Guest               S-1-5-21-1742827456-3351963980-3809373604-501
krbtgt              S-1-5-21-1742827456-3351963980-3809373604-502
SUPPORT_388945a0    S-1-5-21-1742827456-3351963980-3809373604-1001
cda_agent           S-1-5-21-1742827456-3351963980-3809373604-1107

C:\Documents and Settings\Administrator>_
  
```

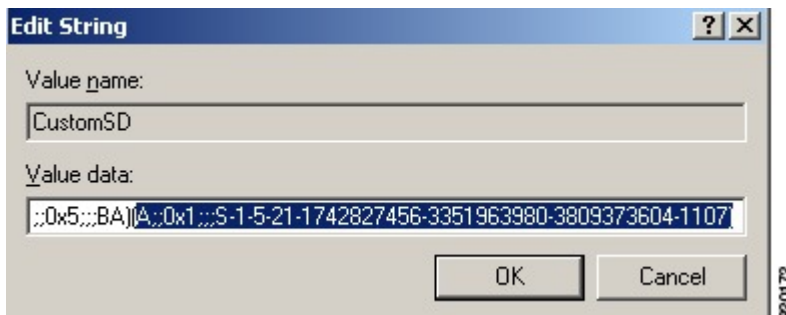
Step 3 Find the SID, open the Registry Editor, and browse to the following location:

```
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 `cda_agent` account (SID - `S-1-5-21-1742827456-3351963980-3809373604-1107`), enter `(A;;0x1;;;S-1-5-21-1742827456-3351963980-3809373604-1107)`.

Figure 32: Edit CustomSD String



- Step 5** Restart the WMI service on the Domain Controller. You can restart the WMI services in the following two ways:
- Run the following commands from the CLI:


```
net stop winmgmt
net start winmgmt
```
 - 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**.

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).

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.
-

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.
- 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 **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.
- 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 in to 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 Settings tab).
- Step 3** Select the root CA certificate in the LDAP identity store.
-

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. RADIUS identity sources use the User Datagram Protocol (UDP) port for authentication sessions. The same UDP port is used for all RADIUS communication.

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 18: Error Handling

Failure Cases	Reasons for Failure
Authentication Failed	<ul style="list-style-type: none"> • User is unknown. • User attempts to log in with an incorrect passcode. • User login hours expired.
Process Failed	<ul style="list-style-type: none"> • 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.
- 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.
 - 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** Click the **Authorization** tab.
 This tab allows you to configure a name that will appear for this single 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. Enter a name for this attribute in the Attribute Name ACS field. The default value is CiscoSecure-Group-Id.
- Step 5** Click **Submit** to save the RADIUS Token identity source.
-

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:

Import the RSA Configuration File

You must import the RSA configuration file to add an RSA identity source in Cisco ISE.

-
- Step 1** Choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID** > **Add**.
 - Step 2** Click **Browse** to choose the new or updated `sdconf.rec` file from the system that is running your client browser. When you create the RSA identity source for the first time, the **Import new `sdconf.rec` file** field will be a mandatory field. From then on, you can replace the existing `sdconf.rec` file with an updated one, but replacing the existing file is optional.

- Step 3** Enter the server timeout value in seconds. Cisco ISE will wait for a response from the RSA server for the amount of time specified before it times out. This value can be any integer from 1 to 199. The default value is 30 seconds.
- Step 4** Check the **Reauthenticate on Change PIN** check box to force a reauthentication when the PIN is changed.
- Step 5** Click **Save**.
Cisco ISE also supports the following scenarios:
- Configuring the Options File for a Cisco ISE Server and Resetting SecurID and sdstatus.12 Files.
 - Configuring Authentication Control Options for RSA Identity Source.

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.
- 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 securid and sdstatus.12 files for that server:
- Click the drop-down arrow and choose **Remove on Submit** in the Reset securid 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.
 - 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 a 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** 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.

-
- Step 1** Choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID**.
- Step 2** Click **Prompts**.
- Step 3** Enter the values as described in RSA SecurID Identity Source Settings.
- Step 4** Click **Submit**.
-

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.

-
- Step 1** Choose **Administration** > **Identity Management** > **External Identity Sources** > **RSA SecurID**.
- Step 2** Click **Prompts**.
- Step 3** Click the **Messages** tab.
- Step 4** Enter the values as described in RSA SecurID Identity Source Settings.
- Step 5** Click **Submit**.
-

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 protects and secures authentication information. It provides encryption functions to protect authentication information passed between the IdP, service provider, and user. SAML SSO can also hide authentication messages passed between the IdP and the service provider from any external user.
- 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.

**Note**

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

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.



Note SAML SSO feature is supported only for Oracle Access Manager (OAM) and Oracle Identity Federation (OIF).

The IdP cannot be added to an identity source sequence (see [Identity Source Sequences](#), on page 316).

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:

```
<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">SignOn 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 in to 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 **Administration > Identity Management > External Identity Sources** .
- Step 3** Click **SAML Id Providers**.
- Step 4** Click **Add**.
- Step 5** In the **SAML Identity Provider** page, enter the following details:

General tab	Id Provider Name—Enter a name for the IdP object. Description—(Optional) Enter the description for the IdP object.
-------------	---

Identity Provider Config tab	<p>Browse—Click this button to import the metadata file of the IdP. Refer to the Identity Provider user documentation for information on how to export the metadata file.</p> <p>After the metadata file is imported into ISE, the following fields are auto-populated:</p> <p>Note All these fields are mandatory. The imported metadata file must contain valid values for all these fields.</p> <p>Provider Id—A unique identifier that identifies the IdP of the user.</p> <p>Logout URL—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.</p> <p>Redirect Param Name—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.</p> <p>If logout does not work as expected, check the Identity Provider documentation for the Logout URL and Redirect Parameter Name.</p> <p>Note Standard SAML v2 logout method is not supported in Cisco ISE.</p> <p>Single Sign On URL—This is the fully-qualified URL of the Single Sign On (SSO) login page of the IdP.</p> <p>Signing Certificate—The IdP sends a public key certificate that service provider uses to verify that SAML responses have been transmitted securely and originate from the IdP.</p>
------------------------------	--

Step 6 Click **Submit**.

Step 7 Go to the Portal Settings page (Guest, Sponsor, 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:

- Guest portal—Choose **Guest Access > Configure > Guest Portals > Create, Edit, or Duplicate > Portal Behavior and Flow Settings > Portal Settings** (see [Portal Settings for Credentialed Guest Portals](#), on page 758).
- Sponsor portal—Choose **Guest Access > Configure > Sponsor Portals > Create, Edit, or Duplicate > Portal Behavior and Flow Settings > Portal Settings** (see [Portal Settings for Sponsor Portals](#), on page 776).
- My Devices portal—Choose **Administration > Device Portal Management > My Devices > Create, Edit, or Duplicate > Portal Behavior and Flow Settings > Portal Settings** (see [Portal Settings for My Devices Portals](#), on page 747).

Note If you have enabled SAML SSO for a Sponsor portal, ensure that the Sponsor groups are linked to an external identity store, such as LDAP or Active Directory.

- Step 8** Click **Save**.
- Step 9** Choose **Administration > Identity Management > External Identity Sources > SAML Id Providers** . Select the IdP that is linked to that portal and click **Edit**.
- Step 10** In the **Service Provider Info** tab, click **Export** to export the service provider metadata file.
- Note** You must re-export the service provider metadata, 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 11** 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 12** 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.
- Note** For the Attribute Mapping option, you must select the sp-attribute-profile to add a mapping attribute for the "username" attribute. For SAML SSO to work as expected, you must define attribute mapping for username attribute. This attribute is included in SAML Assertion and represents unique identifier for the user who logged in. Through this attribute, Cisco ISE identifies the identity of an authenticated user. If username attribute is not provided, the authentication is rejected by ISE.
- Step 13** Click **Portal Test URL** in the ISE portal to confirm whether the IdP is configured properly.
-

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 **Administration > Identity Management > External Identity Sources > SAML Id Providers** .
- Step 2** Check the check box 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.

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)

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 > Authentications to view real-time authentication summary. For more information, see [Recent RADIUS Authentications](#), on page 851.

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.



Configure Guest Access

- [Cisco ISE Guest Services, page 319](#)
- [Guest and Sponsor Accounts, page 320](#)
- [Guest Portals, page 338](#)
- [Sponsor Portals, page 350](#)
- [Monitor Guest and Sponsor Activity, page 354](#)
- [Guest Access Deployment Scenarios, page 356](#)

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 even 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 Services are configured on the following pages:

- [Guest Portals, on page 338](#)
- [Guest Types and User Identity Groups, on page 321](#)
- [Sponsor Portals, on page 350](#)
- [Sponsor Groups, on page 335](#)

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 functionality.

Administration Node

Any configuration changes you make to users or devices on the end-user portals are written to the Administration node.

Policy Services Node

You must run the end-user portals on a Policy Services Node, which handles all session traffic, including: network access, client provisioning, guest services, posture, and profiling. If the Policy Service Node is part of a node group, and the 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 services support various types of users—guests, sponsors, and employees. From the Admin portal, you must define the access privileges and feature support for sponsors. Sponsors then access the Sponsor portal to create and manage guest accounts.

Once their guest accounts are created, guests can use the Sponsored-Guest portal to log in and gain access to the network. Guests can also create their own accounts by registering themselves using the Self-Registered Guest portal and then logging in to the network. Based on the portal configuration, these self-registering guests may need sponsor approval before they can 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 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.

Guest Accounts

Guests typically represent authorized visitors, contractors, customers, or other temporary users who require access to your network. However, 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

Guests typically represent authorized visitors, contractors, customers, or other temporary users who require access to your network. However, 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.

Manage Guest Accounts on the Sponsor Portal

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.

As an ISE administrator, you can access the Sponsor portal through any one of the following ways:

- From the Guest Access menu using the Manage Accounts link—Full access to the default Sponsor portal.
- From the Sponsor portal using a valid Sponsor account—Permissions and restrictions based on the sponsor group to which the sponsor belongs.



Note

An ISE administrator 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.

Step 1

To open the Sponsor Console using the Manage Accounts link—On the Administrators console, click **Guest Access**, then click **Manage Accounts**.

This step requires that you have added the Sponsor Portal URL to your DNS server. If you haven't done that yet, follow the next step.

Step 2

You can also open the Sponsor Console from the Sponsor Portal configuration page. Click **Guest Access > Configure > Sponsor Portal** page, by opening a Sponsor Portal and clicking the **Portal Test URL** link to the right of the Description field.

What to Do Next

Refer to the *Sponsor Portal User Guide for Cisco Identity Services Engine* http://www.cisco.com/c/en/us/td/docs/security/ise/2-1/sponsor_guide/b_spons_SponsorPortalUserGuide_21.html for information on how to use the Sponsor portal.

Guest Types and User Identity Groups

Guest accounts 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. User identity groups are configured in **Administration > Identity Management > Groups > User Identity Groups**. You can delete a user identity group for a guest only by deleting the specific guest type.

For more information, see:

- [User Identity Groups](#), on page 256
- [Create a User Identity Group](#), on page 259

Create or Edit Guest Types

You can edit the default Guest Types and their default access privileges and settings, or you can create new Guest Types. Changes you make will be applied to existing Guest accounts that were created using this Guest Type. Guest users who are logged on will not see these changes until they log off and back on. 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, which are described below.

The navigation path for these settings is **Guest Access > Configure > 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.

Field	Usage Guidelines
Guest type name	Provide a name (from 1-256 characters) that distinguishes this Guest type from the default Guest Types and others that you create.
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, etc.
Language File	Export or Import the language file to use for portals using this Guest Type.
Collect Additional Data	Select custom fields to collect additional information from Guests. Custom fields are managed on Guest Access > Settings > Custom Fields .

Field	Usage Guidelines
Maximum Access Time—Account Duration Starts	<p>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 specified duration time. If the guest user never logs in, the account remains in the Awaiting first login state until the account is removed by the Guest Account Purge Policy. Self-registered and Sponsor-created user's account starts when they create and log on to their account.</p> <p>Note If you use Allow access only on these days and times, then location is used for context of those times. If you don't want FFL access to be based on location, then don't set days and times for access.</p> <p>From sponsor-specified date—Specify the maximum number of days, from 1 to 999, hours or minutes that Guests of this Guest Type can access and stay connected to the network.</p> <p>If you change this setting, your changes will not apply to existing Guest accounts created using this Guest Type.</p>
Allow access only on these days and times	<p>Enter the time ranges and select the days of the week to specify when this Guest Type can access the network. If this guest type remains connected outside these time parameters, they will be logged off. The time ranges are related to the time zones defined by the locations assigned to the guests using this Guest Type.</p> <p>Click the + and - for adding and deleting restricted access times.</p>
Configure guest account Purge Policy	<p>You can schedule an endpoint purge job. The endpoint purge schedule is enabled by default and Cisco ISE deletes endpoints that are older than 30 days. Refer to the Endpoints Purge Settings section for more information.</p>
Login Options—Maximum simultaneous logins	<p>Enter the maximum number of user sessions that this Guest Type can have running concurrently.</p>

Field	Usage Guidelines
When guest exceeds limit	<p>When you select Maximum simultaneous logins, you also must also select the action to take when a user connects after that limit is reached.</p> <p>When the guest exceeds limit</p> <ul style="list-style-type: none"> • Disconnect the oldest connection • Disconnect the newest connection <ul style="list-style-type: none"> ◦ 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 tab.
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 will only affect newly created Guest accounts.
Allow guest to bypass the Guest portal	<p>Allows users to bypass the credentialed Guest captive portal (web authentication page) and access the network by providing credentials to wired and wireless (dot1x) supplicants or VPN clients. Guest accounts go to Active state bypassing the Awaiting Initial Login state and the AUP page, even if it is required.</p> <p>If you do not enable this setting, users must first log in through the credentialed Guest captive portal before they will be able to access other parts of the network.</p>
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 in advance of the expiration.
View messages in	Specify the language to use when displaying email or SMS notifications as you set them up.
Email	Select email as the method used for account expiry notification.
Use customization from	Select email customization from another portal.
Messages	Enter the text to use for account expiry notification.

Field	Usage Guidelines
Copy text from	Reuse email text that you created for another Guest Type for account expiry notification.
Send test email to me at	Ensure that the email notification displays as it should by sending it to your email address.
SMS	Select text (SMS) as the method used for account expiry notification.
Messages	Enter the text to use for account expiry notification.
Copy text from	Reuse text messages that you created for another Guest Type.
Send test SMS to me at	Ensure that the text notification displays as it should by sending it to your cell phone.
These sponsor groups can create this guest type	Select which sponsor groups can create Guest accounts with this Guest Type. If you want to disable use of this Guest Type, do not assign it to any sponsor group. If you want to discontinue use of this Guest Type, delete the sponsor groups listed.

What to Do Next

- Create or modify sponsor groups to use this guest type.
- If appropriate, assign this guest type to self-registering guests in the Self-Registered Guest portal.

Disable Guest Types

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.

Step 1

Do one of the following or both, if appropriate:

- Choose **Guest Access > Configure > Guest Type** and delete all sponsor groups using the specific guest type in **Sponsor Groups**. This action effectively prevents all sponsors from using it to create any new guest accounts.

- Choose **Guest Access > Configure > Guest Portals**. Select the Self-Registered Guest portal that is using the specific guest type and change the assigned guest type for self-registering guests.

Step 2 Click **Save** and then **Close**.

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 Guest users.

When the user logs into the 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, then the Guest user is redirected to an error page. After a configurable period of time, so the user can read the error page, the session is terminated. If the user tries to access the internet again, that user is redirected to the Guest portal's login page.

In an authorization policy, check for a value of true for the attribute *Network Access.SessionLimitExceeded*, and configure the action to take when the maximum number of sessions is reached.

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 logins will not work.

Step 1 Choose **Guest Access > Configure > Guest Type**, and under **Login Options**:

- Enable **Maximum simultaneous logins**. This is already enabled on the default Guest types.
- Select **Disconnect the newest connection**, select **Redirect user to a portal page showing an error message**, and choose the maximum number of simultaneous logins to allow.

Step 2 Choose **Policy > Results**, and create an authorization profile:

- Under Common Tasks, Select **Web Redirection**, then:
 - In the first drop-down, select **Centralized Web Auth**.
 - Enter the **ACL** you created as part of the prerequisite.
 - For **Value**, select any Guest portal.
- Select **Reauthentication**, then:

- 1 In **Timer**, enter the amount of time you would like the error page to appear before redirecting the user to the Guest portal login page.
- 2 In **Maintain Connectivity During Reauthentication**, choose **Default**.

Step 3 Browse to **Policy > Authorization**, 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 **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. If a first login does not happen, on expiry of the specified time period, the guest account is moved to the expired state and is then purged, based on the configured purge policy.
- 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 Guest Types](#).
- When configuring the Sponsor portal for sponsors to use when creating guest accounts. See [Customize Sponsor Portals](#), on page 354.
- When requesting information from self-registering guests using a Self-Registered Guest portal. See [Create a Self-Registered Guest Portal](#), on page 347.

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.

Sponsors can manually send email notifications to guests to deliver their login credentials and password reset instructions. Sponsors can also receive email notifications requiring their approval for self-registering guests.

During the portal configuration, you can choose to automatically send guests email notifications with their login credentials after they successfully register themselves.

-
- Step 1** To specify email settings and configure SMTP servers for all Guest and Sponsor portals, choose **Guest Access > Settings > Guest Email Settings**.
- Step 2** Choose **Administration > System > Settings > SMTP Server** if you want to add more SMTP servers. Configure the SMTP server to enable notifications.
- 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 **Guest Access > 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.
- 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 776.
- 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 336.
- Assign the Guest Locations available to self-registering guests using a Self-Registered Guest portal. See [Create a Self-Registered Guest Portal](#), on page 347.

Rules for Guest Password Policies

Cisco ISE has the following built-in rules for guest 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.

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.

-
- 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.

- 1 Choose **Guest Access > Configure > Sponsored-Guest Portals or Self-Registered Guest Portals > Edit > Portal Page Customization > Error Messages**.
- 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 **Guest Access > 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.

- 1 Choose **Guest Access > Configure > Sponsored-Guest Portals, Self-Registered Guest Portals, Sponsor Portals, or My Devices Portals > Edit > Portal Page Customization > Error Messages**.
- 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 allow sponsors to send SMS notifications to guests whose accounts they have created, you should also 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.

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:
 - **SMS Email Gateway** to send SMS via an email server.
 - **SMS HTTP API** to send SMS via an HTTP API (GET or POST method).

For information about configuring an SMS Email Gateway and an SMS HTTP API gateway, see [SMS Gateway Settings](#), on page 713.

- 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 Guest Types](#).
- 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 347.
- Provide the SMS service providers for sponsors to use when creating guest accounts for guests whose information is available. See [Configure Sponsor Groups](#), on page 336.

Managing Sponsor Accounts

Sponsors are a special type of internal user who can create guest accounts using the Sponsor portal. Like other internal users, 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 in Cisco ISE.

Sponsor Groups

Each sponsor belongs to a sponsor group. The sponsor group configuration defines the permissions and settings for sponsors that are part of that group. Cisco ISE includes these default sponsor groups:

- 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, thereby limiting or expanding functionality of the Sponsor portal. For example:

- You can allow sponsors to create multiple guest accounts in one operation.
- You can restrict sponsors from managing guest accounts created by other sponsors.
- You can restrict sponsors from viewing guest passwords.
- You can grant sponsors the authority to approve or deny requests from self-registering guests.
- You can allow sponsors to delete, suspend, and reinstate guest accounts.

- You can disable a sponsor group to prevent its members from logging in to the Sponsor portal.

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 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.

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 into 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, thereby limiting or expanding functionality of the Sponsor portal. For example:

- You can allow sponsors to create multiple guest accounts in one operation.
- You can restrict sponsors from managing guest accounts created by other sponsors.
- You can restrict sponsors from viewing guest passwords.
- You can grant sponsors the authority to approve or deny requests from self-registering guests.
- You can allow sponsors to delete, suspend, and reinstate guest accounts.

If a sponsor is not a member of any sponsor group, then that sponsor is not permitted to log in to any sponsor portal.

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 **Guest Access > Configure > 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 in to the Sponsor portal. You can delete any of the sponsor groups, except the default sponsor groups provided by Cisco ISE.

Step 1 Enter the **Sponsor group name** and **Description**.

Step 2 Click **Members** to select user (identity) groups and add them as group members of this sponsor group.

Step 3 To specify which guest types can be created by sponsors which are based on this sponsor group, 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, you must save, close, and reopen the sponsor group before you can select that new guest type.

Step 4 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, you must save, close and reopen the sponsor group before you can select that new guest location.

This will not restrict guests from logging in from other locations.

Step 5 Under **Automatic guest notification**, check **Automatically email guests upon account creation if email address is available** if you want to save the your sponsors the step of clicking Notify after creating a user. A window will pop up saying that an email was sent. Checking this also adds a header to the sponsor portal that says **Guest notifications are sent automatically**.

Step 6 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 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.

Step 7 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 8 Under **Sponsor Can** you can provide additional privileges related to guest passwords and accounts to the members of this sponsor group.

- **View guests' passwords**—For guest accounts that they can manage, allow the sponsor to view the passwords.

If the guest has changed the password, the sponsor can no longer view it; unless it was reset by the sponsor to a random password generated by Cisco ISE.

Note If this option is disabled for a sponsor group, the members of that group cannot send email and SMS notifications regarding the login credentials (guest password) for the guest accounts that they manage.

- **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.

- **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.
- **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.
- **Reinstate suspended guest accounts**—For guest accounts that they can manage, allow the sponsor to reinstate suspended accounts.
- **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.

Step 9 Click **Save** and then **Close**.

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 also create their own accounts and 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. 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.

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 **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 **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.
- **Registration code**—Optional. Applies to self-registering guests and is similar to an access code in how it is provided to the self-registering guests. If the Registration code setting is enabled, self-registering guests are prompted to enter it on the Self-Registration form.

The username and password can be provided by a sponsor at your company (for sponsored guests), or a Credentialed Guest portal can be configured to allow guests to register themselves to obtain these credentials.

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.

Configure Periodic AUP Acceptance

Browse to **Policy > Authorization**, 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*).

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.

Task	Hotspot Guest Portal	Sponsored-Guest Portal	Self-Registered Guest Portal
Enable Policy Services, on page 342	Required	Required	Required
Add Certificates for Guest Portals, on page 342	Required	Required	Required
Create External Identity Sources, on page 343	Not applicable	Required	Required
Create Identity Source Sequences, on page 343	Not applicable	Required	Required
Create Endpoint Identity Groups, on page 511	Required	Not required (defined by guest type)	Not required (defined by guest type)
Create a Hotspot Guest Portal, on page 344	Required	Not applicable	Not applicable
Create a Sponsored-Guest Portal, on page 345	Not applicable	Required	Not applicable

Task	Hotspot Guest Portal	Sponsored-Guest Portal	Self-Registered Guest Portal
Create a Self-Registered Guest Portal, on page 347	Not applicable	Not applicable	Required
Authorize Portals, on page 349	Required	Required	Required
Customize Guest Portals, on page 350	Optional	Optional	Optional

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** Chose **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 **Guest Access > Configure > 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 includes certificate authentication profiles that you need for certificate-based authentications.

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 263 for more details).
 - **LDAP** to add an LDAP identity source (see [LDAP](#), on page 295 for more details).
 - **RADIUS Token** to add a RADIUS Token server (see [RADIUS Token Identity Sources](#), on page 303 for more details).
 - **RSA SecurID** to add an RSA SecurID server (see [RSA Identity Sources](#), on page 307 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 312 for more details).
-

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.

-
- 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**.
-

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 will connect to for the Hotspot portal is supported by ISE. See the **Cisco Identity Services Engine Network Component Compatibility** guide for your release, for example, http://www.cisco.com/c/en/us/td/docs/security/ise/2-1/compatibility/ise_sdt.html.

-
- Step 1** Choose **Guest Access > Configure > Guest Portals > Create, Edit or Duplicate**.
- Step 2** If creating a new portal, in the **Create Guest Portal** dialog box, select **Hotspot 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, endpoint identity groups, 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:
- **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 **Guest Access > Configure > 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:
- **Login Page Settings**—Specify guest credential and login guidelines. If you select the **Allow guests to create their accounts** option, users will be able to create their own guest accounts. If this option is not selected, sponsors will be required to create guest accounts.
Note Login Page Settings option will be disabled if you have selected an identity provider (IdP) in the Authentication Method field.
 - **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.
 - **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.
 - **Post-Login Banner Page Settings**—Notify guests of additional information before they are granted network access.
 - **Guest Device Compliance Settings**—Route guests to the Client Provisioning page and require them to first download the posture agent.
 - **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



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.

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.

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 **Guest Access > Configure > 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 758.

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 760.
- **Self-Registration Success Page Settings**—Specify the information that will be displayed to the successfully self-registered guests on the Self-Registration Success page and their guest experience once they are registered in Cisco ISE.
- **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.
- **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.
- **Post-Login Banner Page Settings**—Notify guests of additional information before they are granted network access.
- **Guest Device Compliance Settings**—Route guests to the Client Provisioning page and require them to first download the posture agent.
- **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 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.
- **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.

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 Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

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

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 > Authorization** to create a new authorization policy rule under **Standard** policies. If you enabled Policy Sets, choose **Policy > Policy Set**, pick the Policy Set you plan to use for this portal, expand Authorization Policy, and add a new rule.
- 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.

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.

Configure a Sponsor Portal

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.

-
- Step 1** [Enable Policy Services, on page 351.](#)
 - Step 2** [Add Certificates for Guest Services, on page 351.](#)
 - Step 3** [Create External Identity Sources, on page 352.](#)
 - Step 4** [Create Identity Source Sequences, on page 352.](#)
 - Step 5** [Create a Sponsor Portal, on page 353.](#)
 - Step 6** (Optional) [Customize Sponsor Portals, on page 354.](#)
You can customize the portal if you want to change its appearance.
-

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 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.

-
- Step 1** Chose **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 **Guest Access > Configure > 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.
-

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 includes certificate authentication profiles that you need for certificate-based authentications.

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 263 for more details).
 - **LDAP** to add an LDAP identity source (see [LDAP](#), on page 295 for more details).
 - **RADIUS Token** to add a RADIUS Token server (see [RADIUS Token Identity Sources](#), on page 303 for more details).
 - **RSA SecurID** to add an RSA SecurID server (see [RSA Identity Sources](#), on page 307 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 312 for more details).
-

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 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 776](#). Ensure that the portal name that you use here is not used for any other end-user portals.
- Step 2** Configure the **Login Settings** page, as described in [Login Settings for Sponsor Portals, on page 777](#).
- Step 3** Configure the **Acceptable Use Policy (AUP) Page Settings** page, as described in [Acceptable Use Policy \(AUP\) Settings for Sponsor Portals, on page 778](#).
- Step 4** Configure the **Sponsor Change Password Settings** page, as described in [Set the Guest Password Policy and Expiration, on page 331](#) and in [Rules for Guest Password Policies, on page 330](#).
- Step 5** Configure the **Post-Login Banner Page Settings** page, as described in [Post-Login Banner Settings for Sponsor Portals, on page 779](#).
- Step 6** **Sponsor Portal Application Settings** refers you to the Portal Customization tab if you wish to customize the portal.
- Step 7** Click **Save**.
-

Customize Sponsor 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.

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.

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 Deployment Scenarios

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 (Central WebAuth)**—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.
- **Local Web Authentication (Local WebAuth)**—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 (Device Registration WebAuth)**—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).

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**

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: <https://ip:port/guestportal/gateway?sessionId=NetworkSessionId&portal=<PortalID>&action=cwa>.

- 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.

**Note**

“NetworkAccess:UseCase=GuestFlow” can also apply for Active Directory (AD) and LDAP users who log in as guests.

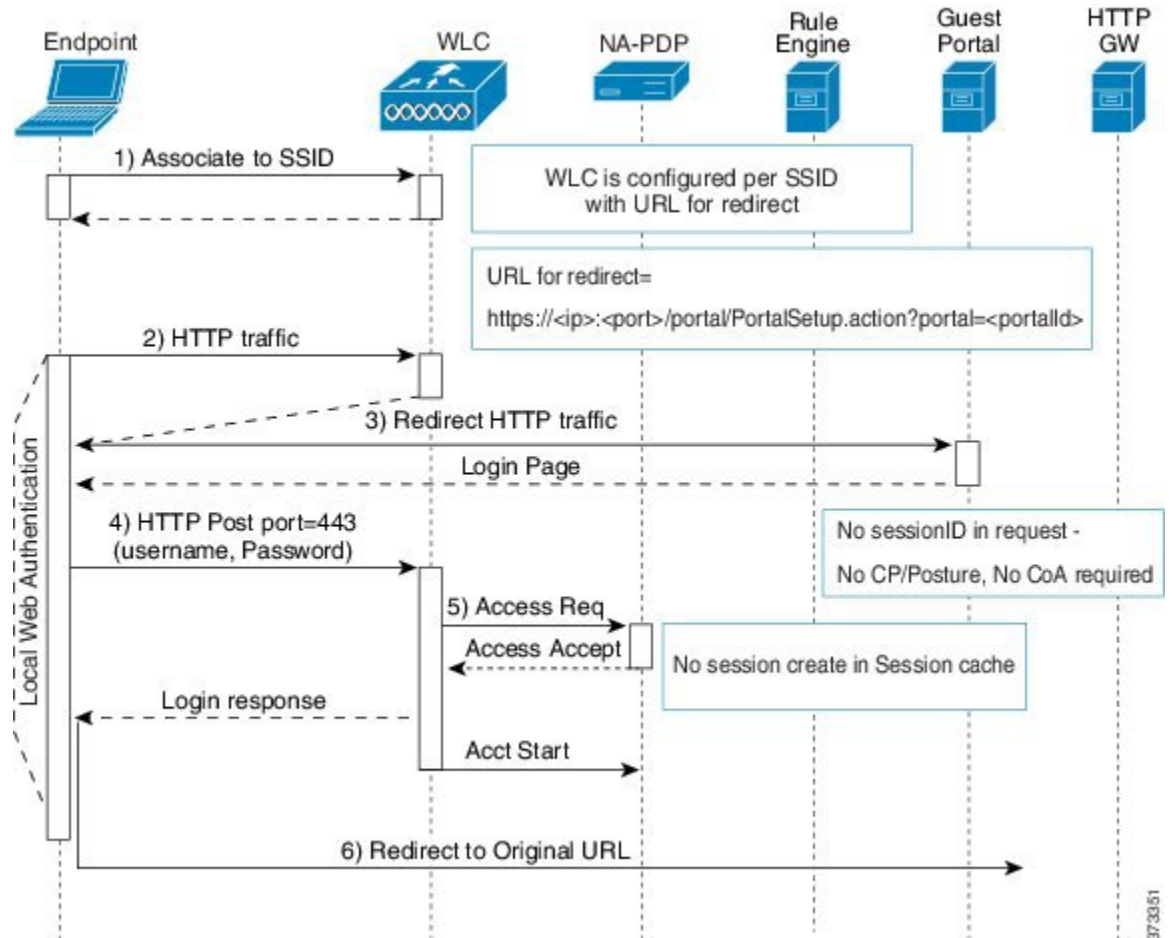
Wireless LAN Controller with Local WebAuth Process

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.

Figure 33: WLC with Local WebAuth Non-Posture Flow



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.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML>
<head>
<title>ISE Guest Portal</title>
<meta Http-Equiv="Cache-Control" Content="no-cache">
<meta Http-Equiv="Pragma" Content="no-cache">
<meta Http-Equiv="Expires" Content="0">
<meta http-equiv="content-type" content="text/html; charset=ISO-8859-1">

<meta http-equiv="REFRESH"
content="0;url=https://ip:port/portal/PortalSetup.action?switch_url=wired">

</HEAD>
<BODY>

<center>
Redirecting ... Login
<br>
<br>
<a href="https://ip:port/portal/PortalSetup.action?switch_url=wired">ISE Guest Portal</a>
</center>

</BODY>
</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:

a.	ip admission proxy http login page file device: <i>login-filename</i>	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.
b.	ip admission proxy http success page file device: <i>success-filename</i>	Specifies the location of the custom HTML file to use in place of the default login success page.
c.	ip admission proxy http failure page file device: <i>fail-filename</i>	Specifies the location of the custom HTML file to use in place of the default login failure page.
d.	ip admission proxy http login expired page file device: <i>expired-filename</i>	Specifies the location of the custom HTML file to use in place of the default login expired page.

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 34: 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:

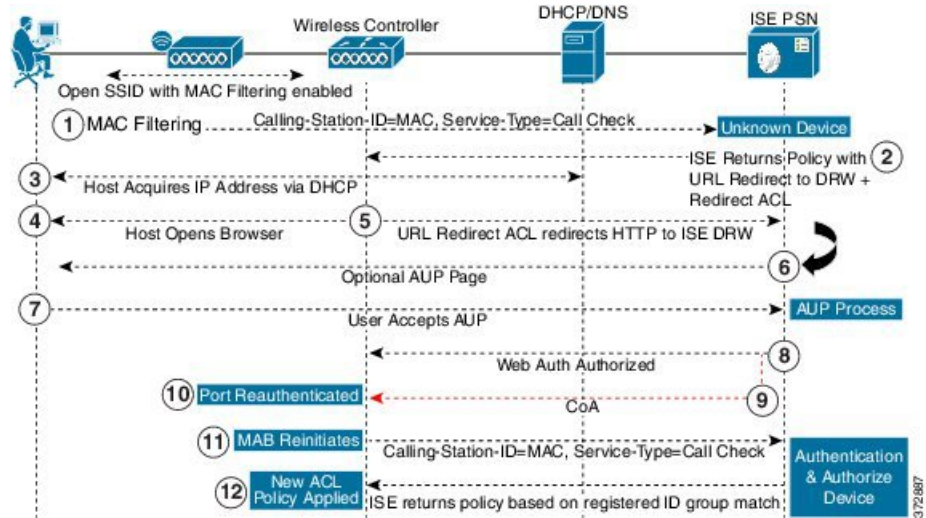
- 1 The network access device (NAD) sends a redirect to the Hotspot Guest portal.
- 2 If the MAC address of the guest device is not in any endpoint identity group or is not marked with an Acceptable Use Policy (AUP) accepted attribute set to true, Cisco ISE responds with a URL redirection specified in 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 34: Wireless Device Registration Web Authentication Flow





Support Device Access

- [Personal Devices on a Corporate Network, page 365](#)
- [Employee Accounts, page 366](#)
- [Personal Device Portals, page 366](#)
- [Support Device Registration Using Native Supplicants, page 369](#)
- [Device Portals Configuration Tasks, page 371](#)
- [Manage Personal Devices Added by Employees, page 382](#)
- [Monitor My Devices Portals and Endpoints Activity, page 383](#)

Personal Devices on a Corporate Network

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. They can also register additional devices up to the maximum limit that you define for their guest type. These devices are registered into endpoint identity groups based on the type of portal used by the guest. For Hotspot Guest portals, the selected endpoint identity group is used, and for credentialed Guest portals, the endpoint identity group is defined by the guest type of the guest.

Users can also add their personal devices to the network using native supplicant provisioning (Bring Your Own Device [BYOD]) or the My Devices portal. You can create native supplicant profiles so that when a user logs in, based on the profile that you associate with that user's authorization requirements, Cisco ISE provides the native supplicant provisioning wizard (via the BYOD portal) required to set up the device for network access.

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.

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 functionality.

Administration Node

Any configuration changes you make to users or devices on the end-user portals are written to the Administration node.

Policy Services Node

You must run the end-user portals on a Policy Services Node, which handles all session traffic, including: network access, client provisioning, guest services, posture, and profiling. If the Policy Service Node is part of a node group, and the 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.

Limit the Number of Personal Devices Registered by Employees

You can allow employees to register between 1 and 100 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.
-

Employee Accounts

When you add users such as employees or contractors to Cisco ISE, either by using external identity stores or by creating internal users, you can authorize them to use their personal devices on your network.

Cisco ISE authenticates these users through a local database, or through external Lightweight Directory Access Protocol (LDAP) or Microsoft Active Directory (AD) identity stores.

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.
- **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 375](#).

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).

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.

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 379.

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.

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.

BYOD Deployment Scenarios for Personal Devices Using Native Supplicants

The BYOD deployment flows that support personal devices using native supplicants 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. At this point, the process diverges based on device type.

Employee Connects to Network

- Single SSID—Employees connect the device to the 802.1X SSID by entering their corporate username and password.
- Dual SSID—Employees connect to the open guest provisioning SSID and are redirected to the credentialed Guest portal. You must check **Allow employees to use personal devices on the network** in **BYOD Settings** in the credentialed Guest portal to enable this functionality.

Employee Credentials Are Authenticated

Cisco ISE authenticates the employee against the corporate Active Directory or other corporate identity stores and provides an authorization policy.

Device Is Redirected to the BYOD Portal

The device is redirected to the BYOD portal. The device's MAC address is automatically preconfigured, but employees can verify and add a description.

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 provides the certificate (if required).
- 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) 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 Google Play. After installing the app, the employee can open NSA and start the setup wizard, which generates authentication parameters and initiates a certificate request (if required) for device certification.

Change of Authorization Issued

Cisco ISE initiates a Change of Authorization (CoA) and connects the MacOS X, Windows, and Android devices 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 must 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).

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 and 8 (excluding RT), Vista, and XP

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 **Guest Access > Configure > 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 will try to reconnect to the Internet automatically. At this point, the IP address or domain name that you enter here will redirect the device to Cisco ISE, which will reinitiate 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.

Task	Blacklist Portal	BYOD Portal	Client Provisioning Portal	MDM Portal	My Devices Portal
Enable Policy Services, on page 373	Required	Required	Required	Required	Required
Add Certificates, on page 373	Required	Required	Required	Required	Required
Create External Identity Sources, on page 374	Not Required	Not Required	Not Required	Not Required	Required
Create Identity Source Sequences, on page 374	Not Required	Not Required	Not Required	Not Required	Required
Create Endpoint Identity Groups, on page 375	Not Required	Required	Not Required	Required	Required
Edit the Blacklist Portal, on page 375	Required	Not applicable	Not applicable	Not applicable	Not applicable
Create a BYOD Portal, on page 376	Not applicable	Required	Not applicable	Not applicable	Not applicable
Create a Client Provisioning Portal, on page 378	Not applicable	Not applicable	Required	Not applicable	Not applicable
Create an MDM Portal, on page 379	Not applicable	Not applicable	Not applicable	Required	Not applicable
Create a My Devices Portal, on page 380	Not applicable	Not applicable	Not applicable	Not applicable	Required
Authorize Portals, on page 381	Not applicable	Required	Required	Required	Not Required

Task	Blacklist Portal	BYOD Portal	Client Provisioning Portal	MDM Portal	My Devices Portal
Customize Device Portals , on page 382	Optional	Optional	Optional	Optional	Optional

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

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** Chose **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 **Administration > Device Portal Management > (any 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 includes certificate authentication profiles that you need for certificate-based authentications.

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 263 for more details).
 - **LDAP** to add an LDAP identity source (see [LDAP](#), on page 295 for more details).
 - **RADIUS Token** to add a RADIUS Token server (see [RADIUS Token Identity Sources](#), on page 303 for more details).
 - **RSA SecurID** to add an RSA SecurID server (see [RSA Identity Sources](#), on page 307 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 312 for more details).
-

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.

-
- 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 ISE and were using Port values outside this range, they are honored until you make any change to this page. If you do change this page, you must 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.

- **Allowed interfaces**—Select the PSN interfaces where this portal can run. 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.
 - The Ethernet interfaces must use IP addresses on different subnets.
 - The interfaces you enable here must be available on all the PSNs that are running portals, 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. If the interface IP is not the same as the domain, then configure **ip host x.x.x.x yyy.domain.com** in the ISE CLI to map your interface IP to FQDN in the certificate.
- **Certificate group tag**—Select the group tag of the certificate group to use for the portal's HTTPS traffic.
- **Display Language**—Specify which language is used in the portal: the user's browser locale setting, with a fallback to another language if a browser locale is not available. Or force the portal to always use one language.

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 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.

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.

-
- Step 1** Choose **Administration > Device Portal Management > Client Provisioning 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 in the Client Provisioning portal during the provisioning process:
- a) On the Client Provisioning page:
 - Checking, Scanning and Compliant—When the posture agent is successfully installed and checks, scans and verifies that the device is compliant with posture requirements.
 - Non-compliant—When the posture agent determines that the device is not compliant with posture requirements.
 - b) On the Client Provisioning (Agent Not Found) page:
 - Agent Not Found—When the posture agent is not detected on the device.
 - Manual Installation Instructions—When devices do not have Java or Active X software installed on them, instructions on how to manually download and install the posture agent.
 - Install, No Java/ActiveX—When devices do not have Java or Active X software installed on them, instructions on how to download and install the Java plug-in.

- **Agent Installed**—When the posture agent is detected on the device, instructions on how to start the posture agent, which checks the device for compliance with posture requirements .

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 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:

- In **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 373
- [Create Endpoint Identity Groups](#), on page 375
- [Authorize Portals](#), on page 381
- [Customize Device Portals](#), on page 382

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.
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, 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.

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 Choose **Policy > Policy Elements > Results > Authorization > Authorization Profiles**.

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:

ip:port = the IP address and port number

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 > Authorization** to create a new authorization policy rule under **Standard** policies. If you enabled Policy Sets, choose **Policy > Policy Set**, pick the Policy Set you plan to use for this portal, expand Authorization Policy, and add a new rule.
- 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.

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 **Administration > Identity Management > 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, if another employee has previously added it such that the device already exists in the Cisco ISE 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 will overwrite 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 you must resolve ownership of the device first. 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.

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 **Administration > Identity Management > Identities > Endpoints**.

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.



Customize End-User Web Portals

- [End-User Portals](#) , page 385
- [Customization of End-User Web Portals](#) , page 385
- [Portal Themes, Images, and Banners](#), page 388
- [Portal Page Titles, Content, and Labels](#), page 389
- [Basic Customization of Portals](#), page 389
- [Advanced Customization of Portals](#) , page 394
- [Customization of a Portal Language File](#), page 412
- [Customization of Guest Notifications, Approvals, and Error Messages](#), page 414

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

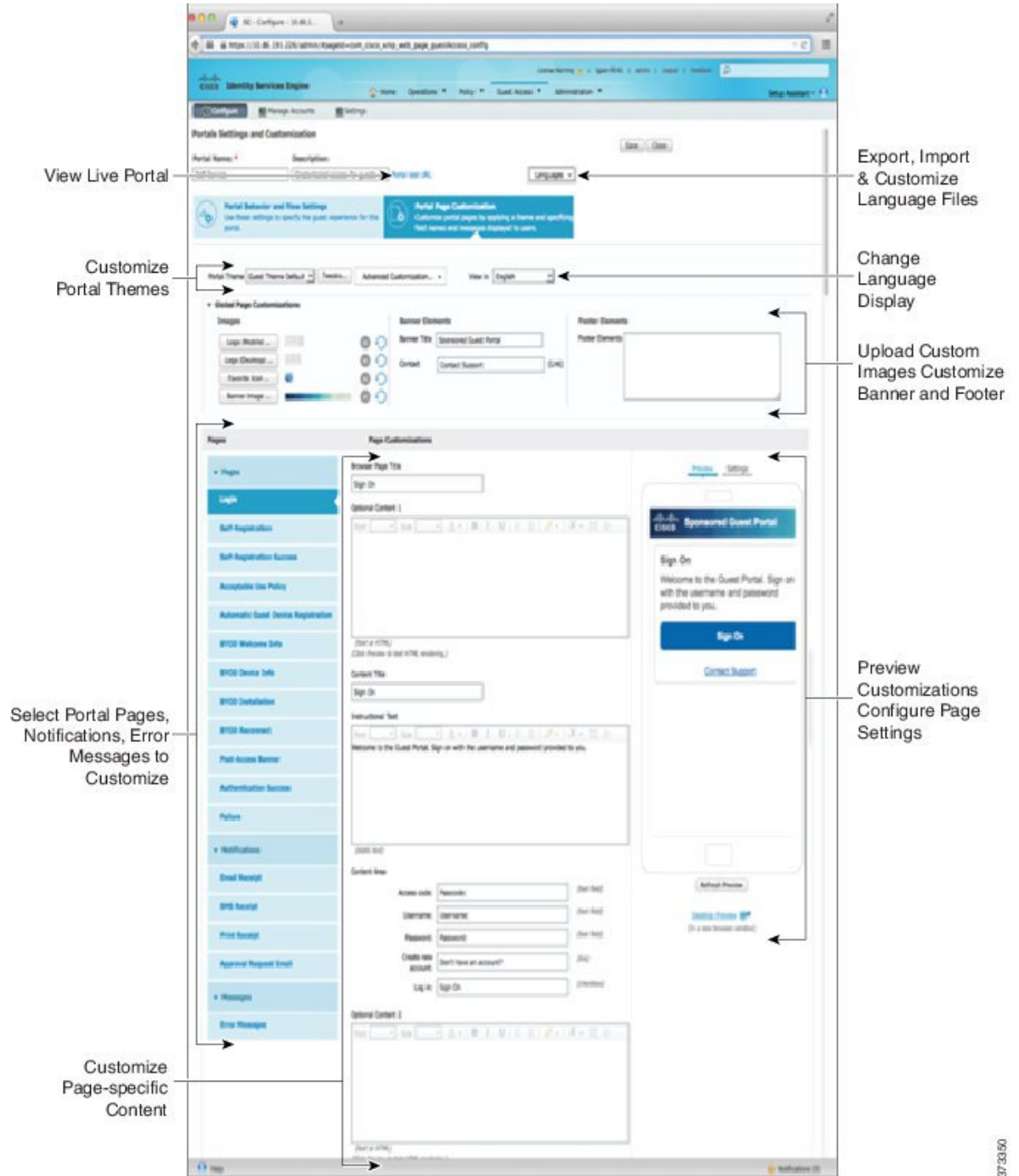
Cisco provides a number of default portals, and lets you edit, duplicate, and create additional portals. You can also fully customize the portal appearance and, therefore, the portal experience. You can customize each individual portal without affecting other portals.

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 http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-43_ISE_Web_Portal_Customization_Options.pdf.

Figure 35: Portal Page Layout for Customization



373360

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:


```
<p style="word-wrap:break-word">
thisisaverylonglineoftextthatwillexceedthewidthofthelacethatyouwanttoputitsousethisstructure
</p>
```
- When you use HTML or javascript to customize portal pages, make sure 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 Themes, Images, and Banners

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:

Banner	1724 X 133
--------	------------

Desktop Logo	86 X 45
Mobile Logo	80 X 35

Note that ISE will resize the images to fit the portal, but images that are too small may not look right after resizing.

If you want to perform advanced customization, such as change the page layout or add 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 on the fly.

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 389](#)
- [Change the Portal Icons, Images, and Logos, on page 391](#)
- [Update the Portal Banner and Footer Elements, on page 391](#)
- [Change the Portal Display Language, on page 390](#)
- [Change the Titles, Instructions, Buttons, and Label Text, on page 392](#)
- [Format and Style Text Box Content, on page 392](#)



Tip

You can [View Your Customization, on page 393](#) 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.

- After changing the colors in a portal theme, if you select another portal theme from the **Portal Theme** drop-down menu, the changes are lost in the original portal theme and it reverts to its default colors.
- If you tweak the colors of a portal theme with an already modified color scheme and then reset its colors before saving it, the color scheme reverts to its default colors and any previous modifications are lost.

Step 1 Navigate to these portals:

- For Guest portals, choose **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
- For Sponsor portals, choose **Guest Access > Configure > Sponsor 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 Guest portals, choose **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization > Global Customization**.
- For Sponsor portals, choose **Guest Access > Configure > Sponsor Portals > Edit > Portal Page Customization > Global Customization**.
- 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.

Step 1

Navigate to these portals:

- For Guest portals, choose **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
- For Sponsor portals, choose **Guest Access > Configure > Sponsor Portals > Edit > Portal Page Customization**.
- For Device portals, choose **Administration > Device Portal Management > (any Portals) > Edit > Portal Page Customization**.

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.

Step 1

Navigate to these portals:

- For Guest portals, choose **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
- For Sponsor portals, choose **Guest Access > Configure > Sponsor Portals > Edit > Portal Page Customization**.
- For Device portals, choose **Administration > Device Portal Management > (any Portals) > Edit > Portal Page Customization**.

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 **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
- For Sponsor portals, choose **Guest Access > Configure > Sponsor 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 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 Guest portals, choose **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
- For Sponsor portals, choose **Guest Access > Configure > Sponsor 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 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.

View Your Customization

You can view how your customization will display to the portal users (guests, sponsors, or employees).

- 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 File Upload

The custom file upload menu lets you upload your own files to the ISE server, which you can use to customize Guest and BYOD portals. The files you upload will be stored on the PSN, and synchronized on all PSNs.

Supported file types are:

- .png, .gif, .jpg, .jpeg - For backgrounds, announcements, advertisements
- .htm, .html, .js, .json - For advanced customization, for example, the portal builder

File sizes are limited to:

- 20 MB per file

- 200 MB total of all files

Uploaded files can be referenced by all portal types, except the admin portal, in the mini-editors under portal page customization. Toggle to the HTML Source view, and create an href to an uploaded file. The path column displays the link to the file, which you can paste into the mini-editor. If the file is an image, when you click the link, it opens a new window that displays the image.

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 399](#), and use it as a base for creating a custom portal theme.
- [Create a Custom Portal Theme CSS File, on page 400](#), by editing the default portal theme and saving it as a new file.
- [Import the Custom Portal Theme CSS File, on page 411](#), 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.

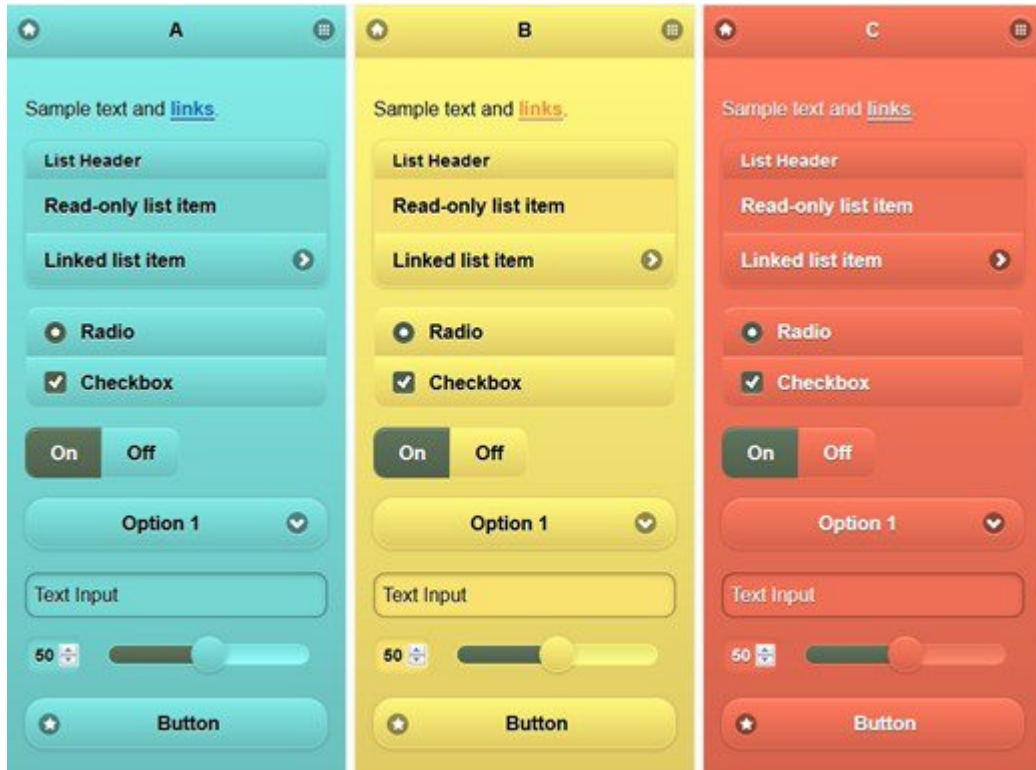
To edit the default Cisco-provided CSS files or create new files based on the CSS classes and structures defined in the default themes, use the required version of [jQuery Mobile ThemeRoller \(Release 1.3.2\)](#).

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.

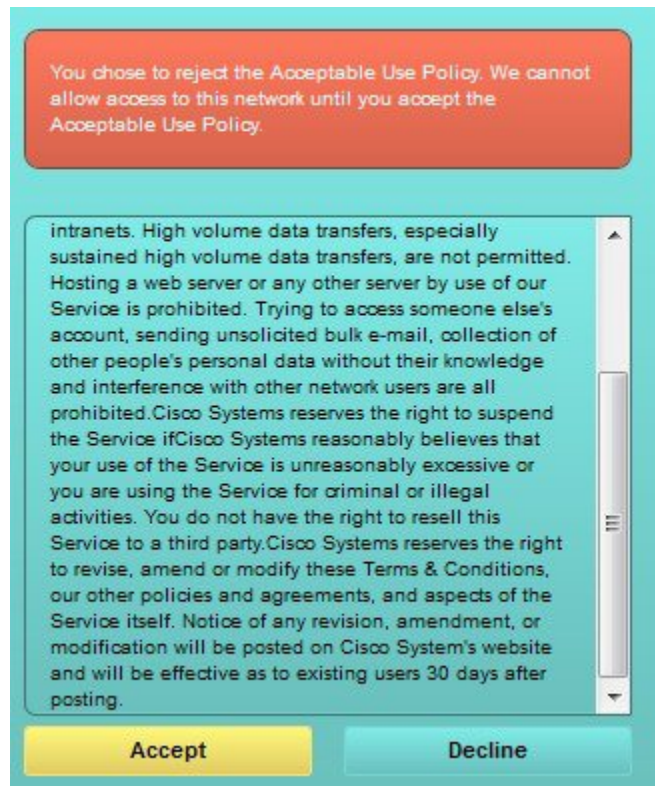
For tutorials on how to use HTML, CSS, and Javascript code to customize the text and content that appears on your portal pages, visit [Code Academy](#).

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.



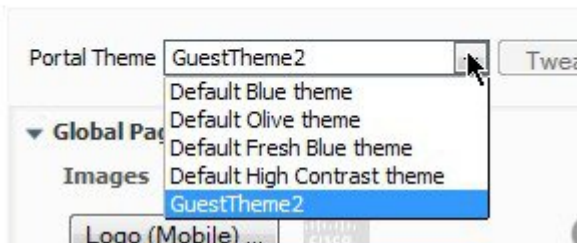
Change Theme Colors with jQuery Mobile

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**.

User Device Type Based Customization

Cisco ISE detects the type of client device used by users (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 into 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 Guest portals, choose **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization > Pages**.
- For Sponsor portals, choose **Guest Access > Configure > Sponsor Portals > Edit > Portal Page Customization > Pages**.
- 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

- You should download to your desktop the *theme.css* file from the portal that you want to customize.
- You should have experience working with HTML, CSS, and Javascript code.
- You should have access to jQuery Mobile ThemeRoller, Release 1.3.2.

-
- Step 1** Import the downloaded portal *theme.css* file contents into the jQuery Mobile ThemeRoller tool.
Tip You can [View Your Customization, on page 412](#) as you make your changes.
- Step 2** (Optional) [Embed Links in Portal Content, on page 400](#)
- Step 3** (Optional) [Insert Variables for Dynamic Text Updates, on page 401](#)
- Step 4** (Optional) [Use Source Code to Format Text and Include Links, on page 402](#)
- Step 5** (Optional) [Add an Image as an Advertisement, on page 403](#)
- Step 6** (Optional) [Customize Greetings Based on Guest Location, on page 406](#)
- Step 7** (Optional) [Customize Greetings Based on User Device Type, on page 407](#)
- Step 8** (Optional) [Set Up Carousel Advertising, on page 404](#)
- Step 9** (Optional) [Modify the Portal Page Layout, on page 408](#)
- 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 **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
 - For Sponsor portals, choose **Guest Access > Configure > Sponsor 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 **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
 - For Sponsor portals, choose **Guest Access > Configure > Sponsor 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:
`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:

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 Guest portals, choose **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
- For Sponsor portals, choose **Guest Access > Configure > Sponsor 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 **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:

```
<p style="text-decoration:underline;">Welcome to Cisco!</p>
```

For example, to include a link using HTML code, enter:

```
<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**.

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 Guest portals, choose **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
- For Sponsor portals, choose **Guest Access > Configure > Sponsor 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 **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.

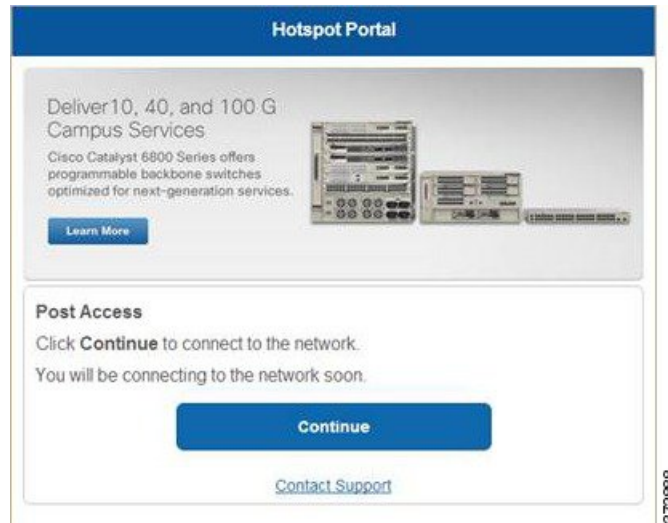
For example, to include a product advertisement and its image using HTML code on the Hotspot Guest portal post-access banner, enter this code in the **Optional Content 1** text box on the **Post-Access Banner** page:

```
<p style="text-decoration:underline;">Optimized for 10/40/100 Campus Services!</p>

```

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 36: Sample Image for an Advertisement



Step 6 Click **Save**.

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 Guest portals, choose **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
- For Sponsor portals, choose **Guest Access > Configure > Sponsor 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 **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:

```
<script>
var currentIndex = 0;
setInterval(changeBanner, 5000);

function changeBanner() {
var bannersArray = ["<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq/
n21v1DrawerContainer.img.jpg/1379452035953.jpg' width='100%' />",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_0/
n21v1DrawerContainer.img.jpg/1400748629549.jpg' width='100%' />",
"<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq_1/
n21v1DrawerContainer.img.jpg/1376556883237.jpg' width='100%' />"
];
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">
<img src='http://www.cisco.com/c/en/us/products/routers/index/_jcr_content/
content_parsys/overview/layout-overview/gd12v2/gd12v2-left/n21v1_cq/
n21v1DrawerContainer.img.jpg/1379452035953.jpg' />
</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:

```
<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 **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
 - For Sponsor portals, choose **Guest Access > Configure > Sponsor 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**:

```
<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 **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
 - For Sponsor portals, choose **Guest Access > Configure > Sponsor 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:

```
<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 brough 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 side bar in the desktop device mode
- A sidebar in the mobile device mode

```
#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 **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
- For Sponsor portals, choose **Guest Access > Configure > 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:

```

<ul data-role="listview">
  <li>Rent a Car</li>
  <li>Top 10 Hotels</li>
  <li>Free Massage</li>

```

```
<li>Zumba Classes</li>  
</ul>
```

Figure 37: View of a Side Bar on a Sample AUP Page (on a Desktop Device)

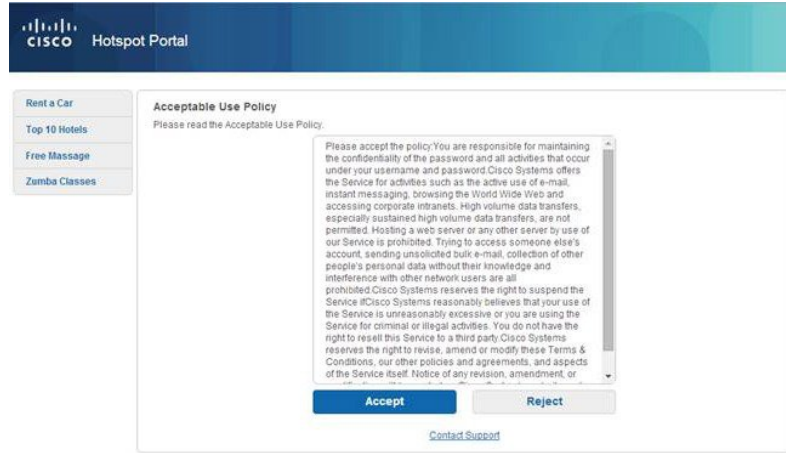
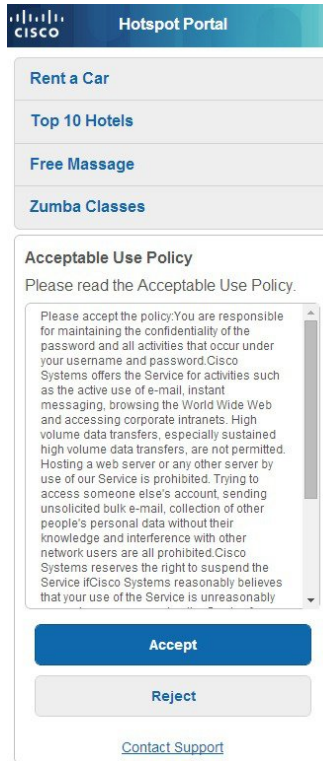


Figure 38: View of a Side Bar on a Sample AUP Page (on a Mobile Device)



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.

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 **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
 - For Sponsor portals, choose **Guest Access > Configure > Sponsor 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 **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 **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization**.
- For Sponsor portals, choose **Guest Access > Configure > Sponsor 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).

- 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.

Customization of a Portal Language File

By default, each portal type supports 15 languages that you can use to display text to guests using the portal. These languages are available as individual property files bundled together in a single zipped language file. Including all the supported languages in a single language file lets you easily use it for customization, translation, and localization purposes.

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.

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:

- For Guest portals, choose **Guest Access** > **Configure** > **Guest Portals** > **Edit** .
- For Sponsor portals, choose **Guest Access** > **Configure** > **Sponsor Portals** > **Edit** .
- For Device portals, choose **Administration** > **Device Portal Management** > **(any Portals)** > **Edit** .

Step 2

Click **Language File** and choose **Export** from the drop-down list.

Step 3

Save the zipped language file to your desktop, for example: Hotspot.zip, Self-Registered.zip, and so on.

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

You must 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, you should 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.
- 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.

Step 1 Navigate to these portals:

- For Guest portals, choose **Guest Access > Configure > Guest Portals > Edit** .
- For Sponsor portals, choose **Guest Access > Configure > 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 **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 **Guest Access > Configure > Sponsor Portals > Edit > Portal Page Customization > Email Receipt or 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 **Guest Access > Configure > 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 **Guest Access > Configure > 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 **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 **Guest Access > Configure > Self-Registered Guest Portals > Edit > Portal Page Customization > Approval Request Email**. Here you can:
- Change the default **Logo** that is specified under **Global Page Customizations**.
 - 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.
 - Preview your customization on all devices using **Send Test Email** to ensure that it appears as it should.
 - Don't forget to click **Save** and then **Close**.
- Step 2** Customize the content of the approval email sent by the Sponsor. Choose **Guest Access > Configure > 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 Guest portals, choose **Guest Access > Configure > Guest Portals > Edit > Portal Page Customizations > Messages > Error Messages**.
 - For Sponsor Portals, choose **Guest Access > Configure > Sponsor Portals > Edit > Portal Page Customizations > Messages > Error Messages**.

- For Device portals, choose **Administration > 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**.
-



PART **V**

Enable and Configure Cisco ISE Services

- [Set Up Policy Conditions, page 421](#)
- [Manage Authentication Policies, page 429](#)
- [Manage Authorization Policies and Profiles, page 455](#)
- [Cisco ISE Endpoint Profiling Policies, page 469](#)
- [Configure Client Provisioning, page 517](#)
- [Configure Client Posture Policies, page 565](#)
- [Cisco TrustSec Policies Configuration, page 587](#)



CHAPTER 18

Set Up Policy Conditions

- [Policy Conditions, page 421](#)
- [Simple and Compound Conditions, page 421](#)
- [Policy Evaluation, page 422](#)
- [Create Simple Conditions, page 422](#)
- [Create Compound Conditions, page 423](#)
- [Profiler Conditions, page 424](#)
- [Posture Conditions, page 425](#)
- [Create Patch Management Conditions, page 427](#)
- [Create Time and Date Conditions, page 428](#)

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:

DEVICE:Model Name Matches Catalyst6K AND Network Access:Use Case Equals Host Lookup.

You cannot delete conditions that are used in a policy or are part of a compound condition.

Policy Evaluation

Typically, 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.

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:
- ```
(InternalUser:IdentityGroup) : Equal : (UserIdentityGroups: Identity Group Name)
```
- Cisco ISE will not accurately resolve Identity Group entries in the following form: (InternalUser:IdentityGroup) : Equal : (Identity Group Name).
- Step 5** Click **Submit** to save the condition.
- 

## 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

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 a 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 811.
  - Step 3** Click **Submit** to save the profiler condition.
  - Step 4** Repeat this procedure to create more conditions.
-

## 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 (process) is running or not running on the client.
- 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.
- 

### 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
- 

### Cisco-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.

### Cisco-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 antispymware products on the clients during posture validation.

The antivirus and antispymware support chart is available on [Cisco.com](https://www.cisco.com).

## 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**.
- 

## 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
  - 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** In the **Patch Management Condition** page, enter the appropriate values in the fields.
  - Step 4** Click **Submit**.
-

## Create Time and Date Conditions

Time and date conditions allow you to limit or extend permission to access to Cisco ISE system resources.

### Before You Begin

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

---

**Step 1** Choose **Policy > Policy Elements > Conditions > 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 19

## Manage Authentication Policies

---

- [Cisco ISE Authentication Policies, page 429](#)
- [Simple Authentication Policies, page 432](#)
- [Rule-Based Authentication Policies, page 434](#)
- [Protocol Settings for Authentication, page 439](#)
- [Network Access Service, page 441](#)
- [Cisco ISE Acting as a RADIUS Proxy Server, page 444](#)
- [Policy Modes, page 446](#)
- [Configure a Simple Authentication Policy, page 447](#)
- [Configure a Rule-Based Authentication Policy, page 447](#)
- [Policy Sets, page 449](#)
- [Authentication Policy Built-In Configurations, page 451](#)
- [View Authentication Results, page 453](#)

### 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.

## 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\_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.

## Supported Authentication Protocols

The following is a list of protocols that you can choose while defining your authentication 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)
- Protected Extensible Authentication Protocol-Transport Layer Security (PEAP-TLS)

## 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.

## Types of Authentication Failures

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. 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.

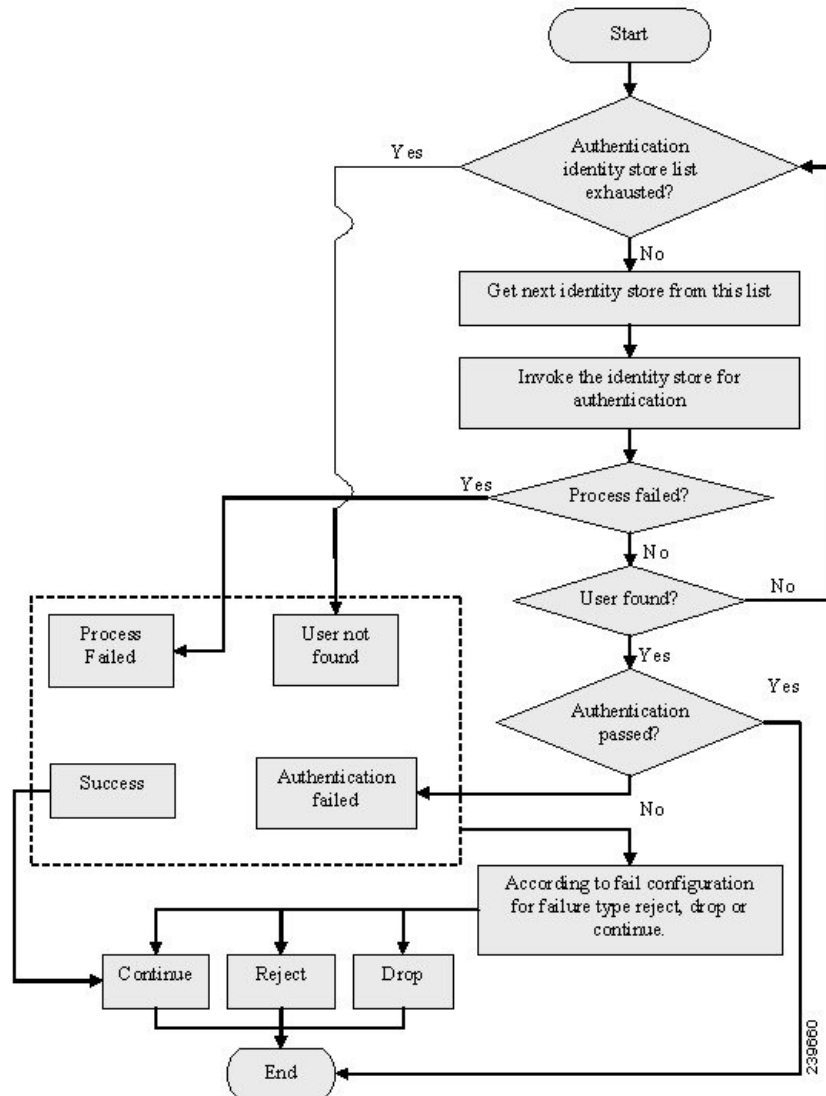
## Simple Authentication Policies

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.

## Simple Authentication Policy Flow

Figure 39: 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).

## 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

## Rule-Based Authentication Policy Flow

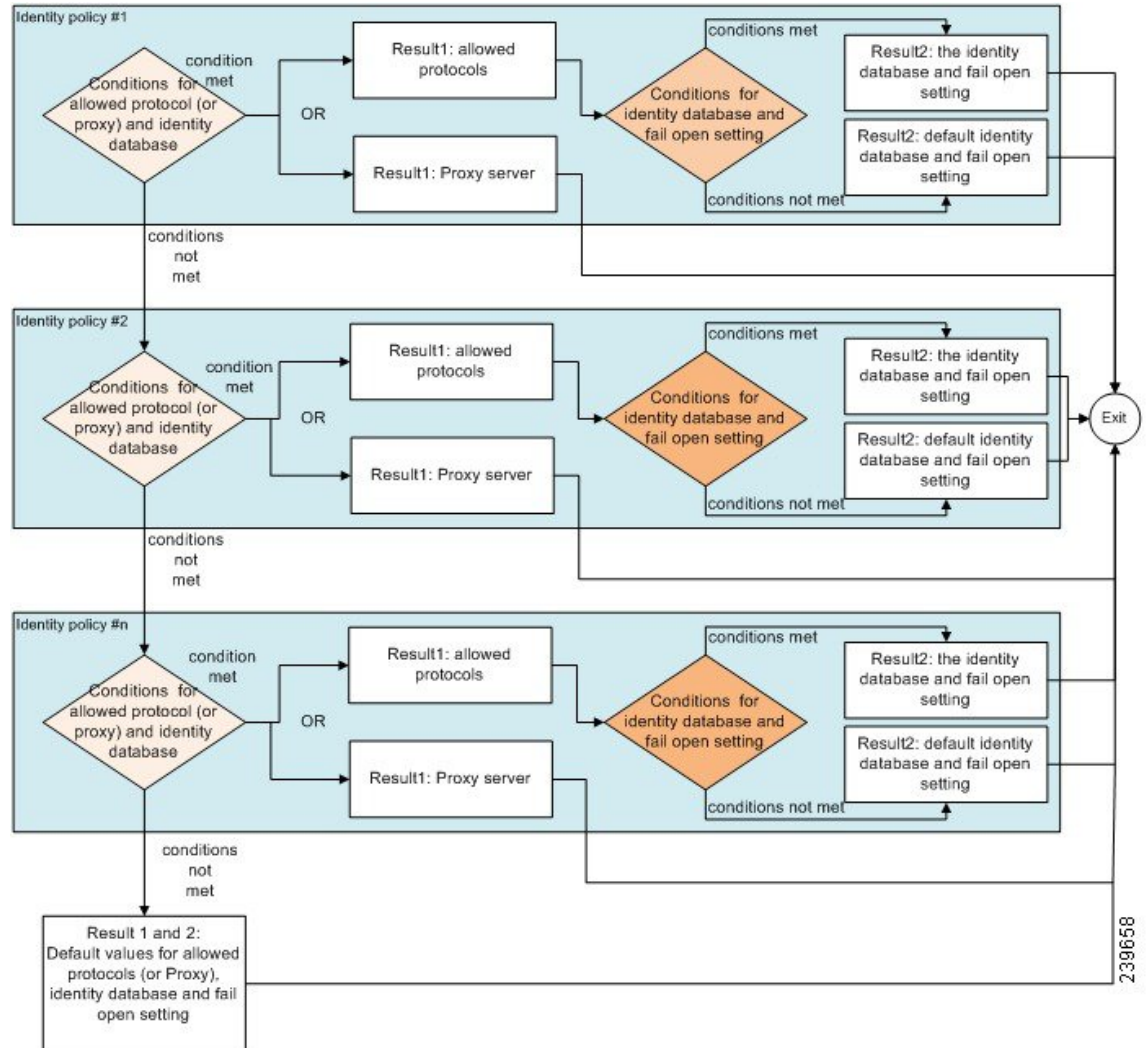
In rule-based policies, you can define multiple rules. The identity database is selected based on the first rule that matches the criteria.

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 40: Rule-Based Authentication Policy Flow**



## Supported Dictionaries for Rule-Based Authentication Policies

Cisco ISE supports the following dictionaries:

- System-defined dictionaries
  - CERTIFICATE
  - DEVICE
  - RADIUS
- RADIUS vendor dictionaries

- Airespace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Microsoft
- Network access

## 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.

| Dictionary | Attributes                                        | Allowed Protocol Rules and Proxy | Identity Rules |
|------------|---------------------------------------------------|----------------------------------|----------------|
| Device     | Device Type (predefined network device group)     | Yes                              | Yes            |
|            | Device Location (predefined network device group) |                                  |                |
|            | Other Custom Network Device Group                 |                                  |                |
|            | Software Version                                  |                                  |                |
|            | Model Name                                        |                                  |                |
| RADIUS     | All attributes                                    | Yes                              | Yes            |

| <b>Dictionary</b> | <b>Attributes</b>                                                                            | <b>Allowed Protocol Rules and Proxy</b> | <b>Identity Rules</b> |
|-------------------|----------------------------------------------------------------------------------------------|-----------------------------------------|-----------------------|
| Network Access    | ISE Host Name                                                                                | Yes                                     | Yes                   |
|                   | AuthenticationMethod                                                                         | No                                      | Yes                   |
|                   | AuthenticationStatus                                                                         | No                                      | No                    |
|                   | CTSDeviceID                                                                                  | No                                      | No                    |
|                   | Device IP Address                                                                            | Yes                                     | Yes                   |
|                   | EapAuthentication (the EAP method that is used during authentication of a user of a machine) | No                                      | Yes                   |
|                   | EapTunnel (the EAP method that is used for tunnel establishment)                             | No                                      | Yes                   |
|                   | Protocol                                                                                     | Yes                                     | Yes                   |
|                   | UseCase                                                                                      | Yes                                     | Yes                   |
|                   | UserName                                                                                     | No                                      | Yes                   |
|                   | WasMachineAuthenticated                                                                      | No                                      | No                    |

| Dictionary                 | Attributes                            | Allowed Protocol Rules and Proxy | Identity Rules |
|----------------------------|---------------------------------------|----------------------------------|----------------|
| Certificate                | Common Name                           | No                               | Yes            |
|                            | Country                               |                                  |                |
|                            | E-mail                                |                                  |                |
|                            | LocationSubject                       |                                  |                |
|                            | Organization                          |                                  |                |
|                            | Organization Unit                     |                                  |                |
|                            | Serial Number                         |                                  |                |
|                            | State or Province                     |                                  |                |
|                            | Subject                               |                                  |                |
|                            | Subject Alternative Name              |                                  |                |
|                            | Subject Alternative Name - DNS        |                                  |                |
|                            | Subject Alternative Name - E-mail     |                                  |                |
|                            | Subject Alternative Name - Other Name |                                  |                |
|                            | Subject Serial Number                 |                                  |                |
|                            | Issuer                                |                                  |                |
|                            | Issuer - Common Name                  |                                  |                |
|                            | Issuer - Organization                 |                                  |                |
|                            | Issuer - Organization Unit            |                                  |                |
|                            | Issuer - Location                     |                                  |                |
|                            | Issuer - Country                      |                                  |                |
| Issuer - Email             |                                       |                                  |                |
| Issuer - Serial Number     |                                       |                                  |                |
| Issuer - State or Province |                                       |                                  |                |
| Issuer - Street Address    |                                       |                                  |                |

| Dictionary | Attributes                | Allowed Protocol Rules and Proxy | Identity Rules |
|------------|---------------------------|----------------------------------|----------------|
|            | Issuer - Domain Component |                                  |                |
|            | Issuer - User ID          |                                  |                |

## Protocol Settings for Authentication

You must define global protocol settings in Cisco ISE before you can use these protocols to process an authentication request. 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.

### Guidelines for Using EAP-FAST as Authentication 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.

## 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.
- 

## 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**.
- 

## 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.

- 
- Step 1** Choose **Administration** > **System** > **Settings**.
  - Step 2** From the Settings navigation pane on the left, click **Protocols**.
  - Step 3** Choose **PEAP**.
  - Step 4** Enter the details as required to define the PEAP protocol.
  - Step 5** Click **Save** to save the PEAP settings.
- 

## 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.

- 
- Step 1** Choose **Administration** > **System** > **Settings**.
  - Step 2** From the Settings navigation pane, click **Protocols**.
  - Step 3** Choose **RADIUS**.
  - Step 4** Enter the details as required to define the RADIUS settings.
  - Step 5** Click **Save** to save the settings.
- 

## 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.

### 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.
-



## 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 an Allowed Protocol service based on the type of MAC authentication used by the non-Cisco device (PAP, CHAP, or EAP-MD5).
- Choose **Policy > Policy Elements > Results > Authentication > Allowed Protocols**
  - Enter a name for the Allowed Protocol service. For example, MAB for NonCisco Devices.
  - Select the protocol based on the MAC authentication type used by the non-Cisco device:
    - PAP—Check the Allow PAP/ASCII check box and check the Detect PAP as Host Lookup check box.
    - CHAP—Check the Allow CHAP check box and check the Detect CHAP as Host Lookup check box.
    - EAP-MD5—Check the Allow EAP-MD5 check box and check Detect EAP-MD5 as Host Lookup check box.

For each of the protocol listed above, it is recommended to check the following check boxes:

    - Check Password—Enable this for checking of the trivial MAB password to authenticate the sending network device.
    - Check Calling-Station-Id equals MAC address—Enable this as an extra security check, when Calling-Station-Id is being sent.
- Step 3** Configure an authentication policy rule for enabling MAB from non-Cisco devices.
- Choose **Policy > Authentication**.
  - Select the Rule-Based authentication policy.
  - Insert a new rule for MAB.
  - Select the Allowed Protocol service (MAB for NonCisco Devices) that you created in Step 2 in this rule.
  - Select the Internal Endpoints database as the Identity Source in this rule.
  - Save the authentication policy.
- 

## 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 an Allowed Protocol service based on the type of MAC authentication used by the Cisco device (PAP, CHAP, or EAP-MD5).
- Choose **Policy > Policy Elements > Results > Authentication > Allowed Protocols**
  - Enter a name for the Allowed Protocol service. For example, MAB for Cisco Devices.

- c) Check the Process Host Lookup check box.
- d) Select the protocol based on the MAC authentication type used by the Cisco device:
  - PAP—Check the Allow PAP/ASCII check box and check the Detect PAP as Host Lookup check box.
  - CHAP—Check the Allow CHAP check box and check the Detect CHAP as Host Lookup check box.
  - EAP-MD5—Check the Allow EAP-MD5 check box and check Detect EAP-MD5 as Host Lookup check box.

For each of the protocol listed above, it is recommended to check the following check boxes:

  - Check Password—Enable this for checking of the trivial MAB password to authenticate the sending network device.
  - Check Calling-Station-Id equals MAC address—Enable this as an extra security check, when Calling-Station-Id is being sent.
- e) Save the Allowed Protocol service.

**Step 3**

Configure an authentication policy rule for enabling MAB from Cisco devices.

- a) Choose **Policy > Authentication**.
- b) Select the Rule-Based authentication policy.
- c) Insert a new rule for MAB.
- d) Select the Allowed Protocol service (MAB for Cisco Devices) that you created in Step 2 in this rule.
- e) Select the Internal Endpoints database as the Identity Source in this rule.
- f) Save the authentication policy.

## 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.
- 

## 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.

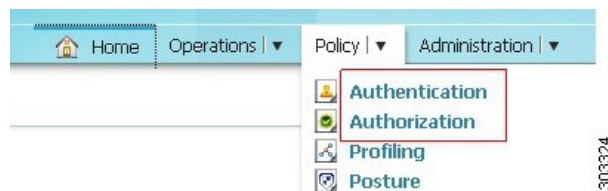
- 
- Step 1** Choose **Administration** > **Network Resources** > **RADIUS Server Sequences**.
- Step 2** Click **Add**.
- Step 3** Enter the values as required.
- Step 4** Click **Submit** to save the RADIUS server sequence to be used in policies.
-

## 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.

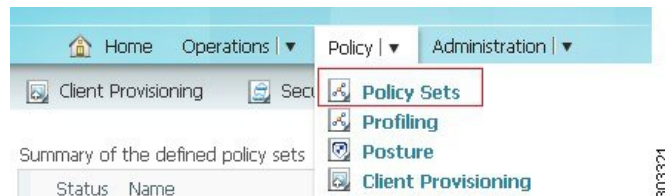
- Simple Mode—If you select Simple mode, you can define authentication and authorization policies separately in the Policy menu.

**Figure 41: 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 42: 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.

- 
- Step 1** Choose **Policy** > **Authentication**.
- Step 2** Click **OK** on the message that appears.
- Step 3** Enter the values as required.
- Step 4** Click **Save** to save your simple authentication policy.
- 

## 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.
-

## 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:

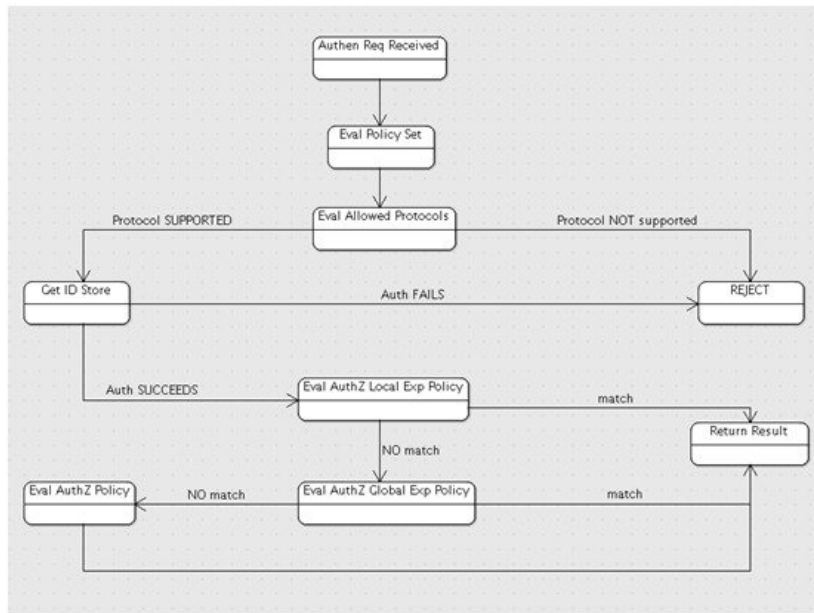
- Airspace
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- Device, Microsoft
- NetworkAccess
- RADIUS

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.

## Policy Set Evaluation Flow

**Figure 43: 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.

## Guidelines for Creating Policy Sets

The following are the guidelines for creating policy sets:

- Rules should be specified with names, conditions, and results. You cannot save a policy set as long as all the authentication and authorization rules are not defined.
- You can duplicate rules as long as they are from the same rule type (authentication or authorization) and only from the same policy set.
- Rules cannot be shared by different policy sets; each policy set has its own rule, however conditions can be shared in case you use the condition library.



## 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**.

- 
- Step 1** Choose **Policy > Policy Sets**.
  - Step 2** Click the **Default** policy. The default policy is displayed in the right.
  - Step 3** Click the plus (+) sign on top and choose **Create Above**.
  - Step 4** Enter the name, description and a condition for this group policy.
  - Step 5** Define the authentication policy.
  - Step 6** Define the authorization policy.
  - 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.
- 

## Authentication Policy Built-In Configurations

Cisco ISE is packaged with several default configurations that are part of common use cases.

**Table 19: Authentication Policy Configuration Defaults**

| Name                                                    | Path in the User Interface                                   | Description                                                                                                  | Additional Information                                                                                |
|---------------------------------------------------------|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
| Default Network Access Allowed Protocols Access Service | Policy > Policy Elements > Configuration > Allowed Protocols | This default is the built-in network access allowed protocols service to be used in authentication policies. | You can use this access service for wired and wireless 802.1X, and wired MAB authentication policies. |

| Name                                                        | Path in the User Interface                                                   | Description                                                                                                                                                                                                              | Additional Information                                                                                                                                                                                                                                      |
|-------------------------------------------------------------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Wired 802.1X Compound Condition                             | Policy > Policy Elements > Conditions > Authentication > Compound Conditions | This compound condition checks for the following attributes and values: <ul style="list-style-type: none"> <li>• RADIUS:Service-Type equals Framed</li> <li>• RADIUS:NAS-Port-Type equals Ethernet</li> </ul>            | 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.                                               |
| Wireless 802.1X Compound Condition                          | Policy > Policy Elements > Conditions > Authentication > Compound Conditions | This compound condition checks for the following attributes and values: <ul style="list-style-type: none"> <li>• RADIUS:Service-Type equals Framed</li> <li>• RADIUS:NAS-Port-Type equals Wireless-IEEE802.11</li> </ul> | 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.                                         |
| Wired MAB Compound Condition                                | Policy > Policy Elements > Conditions > Authentication > Compound Conditions | This compound condition checks for the following attributes and values: <ul style="list-style-type: none"> <li>• RADIUS:Service-Type equals Call-Check</li> <li>• RADIUS:NAS-Port-Type equals Ethernet</li> </ul>        | 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.                                                     |
| Catalyst Switch Local Web Authentication Compound Condition | Policy > Policy Elements > Conditions > Authentication > Compound Conditions | This compound condition checks for the following attributes and values: <ul style="list-style-type: none"> <li>• RADIUS:Service-Type equals Outbound</li> <li>• RADIUS:NAS-Port-Type equals Ethernet</li> </ul>          | 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. |

| Name                                                                      | Path in the User Interface                                                   | Description                                                                                                                                                                                                                       | Additional Information                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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: <ul style="list-style-type: none"> <li>• RADIUS:Service-Type equals Outbound</li> <li>• RADIUS:NAS-Port-Type equals Wireless-IEEE802.11</li> </ul>        | 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.                                                                                                                                                                            |

## 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** Choose **Operations** > **Authentications** to view real-time authentication summary.

**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 that is similar to the one shown in the figure 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. It provides at-a-glance information about authentications and authentication failures in the Authentications dashlet.

The Authentications dashlet provide the following statistical information about the RADIUS 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.

## 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



## CHAPTER 20

# Manage Authorization Policies and Profiles

---

- [Cisco ISE Authorization Policies, page 455](#)
- [Cisco ISE Authorization Profiles, page 455](#)
- [Default Authorization Policy, Rule, and Profile Configuration, page 459](#)
- [Configure Authorization Policies, page 462](#)
- [Permissions for Authorization Profiles, page 464](#)
- [Downloadable ACLs, page 465](#)
- [Machine Access Restriction for Active Directory User Authorization, page 467](#)

## 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

Network 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

Profiles consist of attributes chosen from a set of resources, which are stored in a dictionary and these are returned when the compound condition for the specific authorization policy matches. Because authorization policies can include compound conditions mapping to a single network service rule, these can also include a list of authorization checks.

For simple scenarios, all authorization checks are made using the AND Boolean operator within the rule. For advanced scenarios, any type of authorization verification expression can be used, but all these 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.

## 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 ACL (DACLS).

### Network Authorization

Authorization is an important requirement to ensure which users can access the Cisco ISE network and its resources. Network authorization controls user access to the network and its resources and what each user can do on the system with those resources. The Cisco ISE network defines 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:

- A profile name
- A profile description

- An associated DACL
- An associated VLAN
- An associated SGACL
- Any number of other dictionary-based attributes

## 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 policies 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 both simple and compound 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.
  - Numeric characters: 0-9.
- 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.
  - Numeric characters: 0-9.
- 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).

- Make sure that you click Save to save the new or modified policy or profile in the Cisco ISE database.

## Default Authorization Policy, Rule, and Profile Configuration

The Cisco ISE software comes installed with a number of preinstalled default conditions, rules, and profiles that provide common settings that make it easier for you to create the rules and policies required in Cisco ISE authorization policies and profiles.

The table describes built-in configuration defaults that contain specified values in Cisco ISE.

**Table 20: Authorization Policy, Profile, and Rule Configuration Defaults**

| Name                                                   | Path in the User Interface                                                  | Description                                                                                                                                                                                             | Additional Information                                                                                                                                                                                                                                                         |
|--------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Authorization Policy Configuration Defaults            |                                                                             |                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                |
| Default Compound Conditions for Authorization Policies | Policy > Policy Elements > Conditions > Authorization                       | These are preinstalled configuration defaults for conditions, rules, and profiles to be used in authorization policies.                                                                                 | You can use the related attributes for creating authorization policies: <ul style="list-style-type: none"> <li>• Wired 802.1x</li> <li>• Wired MAB</li> <li>• Wireless 802.1x</li> <li>• Catalyst Switch Local Web authentication</li> <li>• WLC Web authentication</li> </ul> |
| Wired MAB Compound Condition                           | Policy > Policy Elements > Conditions > Authorization > Compound Conditions | This compound condition checks for the following attributes and values: <ul style="list-style-type: none"> <li>• RADIUS:Service-Type = Call-Check</li> <li>• RADIUS:NAS-Port-Type = Ethernet</li> </ul> | This compound condition is used in the Wired MAB authorization policy. Any request that matches the criteria specified in this policy would be evaluated based on the Wired MAB authorization policy.                                                                          |

| Name                                         | Path in the User Interface                                                     | Description                                                                                                                                                                                                                                                                                                                                              | Additional Information                                                                                                                                                                                                   |
|----------------------------------------------|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Wireless 802.1X Compound Condition           | Policy > Policy Elements > Conditions > Authorization > Compound Conditions    | This compound condition checks for the following attributes and values: <ul style="list-style-type: none"> <li>• RADIUS:Service-Type = Framed</li> <li>• RADIUS:NAS-Port-Type = Wireless-IEEE802.11</li> </ul>                                                                                                                                           | This compound condition is used in the Wireless 802.1X authorization policy.<br><br>Any request that matches the criteria specified in this policy would be evaluated based on the Wireless 802.1X authorization policy. |
| Authorization Profile Configuration Defaults |                                                                                |                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                          |
| Blacklist_Access                             | Policy > Policy Elements > Results > Authorization Profiles > Blacklist_Access | This authorization profile rejects access to devices that are blacklisted. All blacklisted devices are redirected to the following URL:<br><a href="http://localhost:8080/portal/portal.html">http://localhost:8080/portal/portal.html</a>                                                                                                               | This default authorization profile is applied for all endpoints that are declared as “lost” in the My Devices Portal.                                                                                                    |
| Cisco_IP_Phones                              | Policy > Policy Elements > Results > Authorization Profiles > Cisco_IP_Phones  | This authorization profiles uses a configuration default profile with the following values: <ul style="list-style-type: none"> <li>• Name: Cisco IP Phones</li> <li>• DACL: PERMIT_ALL_TRAFFIC</li> <li>• VSA: ciscoav-pair-device-traffic-class-voice</li> </ul> This profile will evaluate requests that match the criteria specified in this profile. | This default authorization profile uses the DACL and vendor-specific attribute (VSA) to authorize all “voice” traffic (PERMIT_ALL_TRAFFIC).                                                                              |
| Authorization Policy Configuration Defaults  |                                                                                |                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                          |
| Wired 802.1X Compound Condition              | Policy > Policy Elements > Conditions > Authorization > Compound Conditions    | This compound condition checks for the following attributes and values: <ul style="list-style-type: none"> <li>• RADIUS:Service-Type = Framed</li> <li>• RADIUS:NAS-Port-Type = Ethernet</li> </ul>                                                                                                                                                      | This compound condition is used in the Wired 802.1X authorization policy.<br><br>Any request that matches the criteria specified in this policy would be evaluated based on the Wired 802.1X authorization policy.       |

| Name                                                                      | Path in the User Interface                                                  | Description                                                                                                                                                                                                                                                                                                             | Additional Information                                                                                                                      |
|---------------------------------------------------------------------------|-----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Catalyst Switch Local Web Authentication Compound Condition               | Policy > Policy Elements > Conditions > Authorization > Compound Conditions | <p>This compound condition checks for the following attributes and values:</p> <ul style="list-style-type: none"> <li>• RADIUS:Service-Type = Outbound</li> <li>• RADIUS:NAS-Port-Type = Ethernet</li> </ul>                                                                                                            | To use this compound condition, you must create an authorization policy that would check for this condition.                                |
| Wireless Lan Controller (WLC) Local Web Authentication Compound Condition | Policy > Policy Elements > Conditions > Authorization > Compound Conditions | <p>This compound condition checks for the following attributes and values:</p> <ul style="list-style-type: none"> <li>• RADIUS:Service-Type = Outbound</li> <li>• RADIUS:NAS-Port-Type = Wireless-IEEE802.11</li> </ul>                                                                                                 | To use this compound condition, you must create an authorization policy that would check for this condition.                                |
| Black List Default Authorization Rule                                     | Policy > Authorization Policy                                               | <p>This authorization policy uses a configuration default rule with the following values:</p> <ul style="list-style-type: none"> <li>• Rule Name: Black List Default</li> <li>• Endpoint Identity Group: Blacklist</li> <li>• Conditions: Any</li> <li>• Permissions/Authorization Profile: Blacklist_Access</li> </ul> | This default rule is designed to appropriately provision “lost” user devices until they are either removed from the system or “reinstated.” |

| Name                                        | Path in the User Interface    | Description                                                                                                                                                                                                                                                                                                                 | Additional Information                                                                                             |
|---------------------------------------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Profiled Cisco IP Phones Authorization Rule | Policy > Authorization Policy | This authorization policy uses a configuration default rule with the following values: <ul style="list-style-type: none"> <li>• Rule Name: Profiled Cisco IP Phones</li> <li>• Endpoint Identity Group: Cisco-IP-Phones</li> <li>• Conditions: Any</li> <li>• Permissions/Authorization Profile: Cisco_IP_Phones</li> </ul> | This default rule uses Cisco IP Phones as its default endpoint identity group and the values listed in this table. |
| Authorization Rule Configuration Defaults   |                               |                                                                                                                                                                                                                                                                                                                             |                                                                                                                    |
| Default Authorization Rule                  | Policy > Authorization Policy | This authorization policy uses a configuration default rule with the following values: <ul style="list-style-type: none"> <li>• Rule Name: Default</li> <li>• Endpoint Identity Group: Any</li> <li>• Conditions: Any</li> <li>• Authorization Profile: PermitAccess</li> </ul>                                             | This default rule uses “any” as its default endpoint identity group and the values listed in this 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. 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.
- Step 4** Click **Done**.
- Step 5** Click **Save** to save your changes to the Cisco ISE system database and create this new authorization policy.
- 

## 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 endpointIDgroup 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”.

## 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.

## 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
- Are aware of configuration default values that are described in the related links.

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.

## 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, ! # \$ % & ' ( ) \* + , - . / ; = ? @ \_ {.
  - Step 4** Click **Submit** to save your changes to the Cisco ISE system database to create an authorization profile.
- 

## Downloadable ACLs

You can define DACLs for the Access-Accept message to return. Use ACLs to prevent unwanted traffic from entering the network. ACLs can filter source and destination IP addresses, transport protocols, and more by using the RADIUS protocol.

After you create DACLs as named permission objects, you can add them to authorization profiles, which you can then specify as the result of an authorization policy.

You can duplicate a DACL if you want to create a new DACL that is the same, or similar to, an existing downloadable ACL.

After duplication is complete, you access each DACL (original and duplicated) separately to edit or delete them.



### Note

While creating DACL, the keyword **Any** must be the source in all ACE in 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.

---

## Configure Permissions for Downloadable ACLs

- 
- Step 1** Choose **Policy > Policy Elements > Results > Authorization > Downloadable ACLs**.
  - Step 2** Click the action icon and select **Create DACL** or click **Add** in the DACL Management page.
  - Step 3** Enter the desired values for the DACL. Supported characters for the name field are: space, ! # \$ % & ' ( ) \* + , - . / ; = ? @ \_ {.
  - Step 4** Click **Submit**.
- 

## Supported Downloadable ACL Format for Inline Posture Node

The following format is supported for DACLs:

ACTION PROTOCOL SOURCE\_SUBNET WILDCARD\_MASK [OPERATOR [ PORT ]] DEST\_SUBNET  
WILDCARD\_MASK [OPERATOR [ PORT ]] [ICMP\_TYPE\_CODE]

**Table 21: DACL Format - Options**

| Option        | Description                                                                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ACTION        | Specifies whether the policy element permissions should permit or deny access.                                                                                           |
| PROTOCOL      | Specifies any one of the following protocols: <ul style="list-style-type: none"> <li>• ICMP</li> <li>• UDP</li> <li>• TCP</li> <li>• IP</li> </ul>                       |
| SOURCE_SUBNET | Specifies the source subnet format as 'any'.                                                                                                                             |
| DEST_SUBNET   | Specifies any one of the following destination subnet formats: <ul style="list-style-type: none"> <li>• any</li> <li>• host x.x.x.x</li> <li>• &lt;subnet&gt;</li> </ul> |
| WILDCARD_MASK | Specifies the inverse of the subnet mask. For example, 0.0.0.255.                                                                                                        |
| OPERATOR      | Specifies any one of the following operators: <ul style="list-style-type: none"> <li>• eq</li> <li>• lt</li> <li>• gt</li> <li>• neq</li> <li>• range</li> </ul>         |
| PORT          | Specifies the port. The valid range is from 1 to 65535.                                                                                                                  |



| Option         | Description                                                                                                                                                                                                                  |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ICMP_TYPE_CODE | Specifies any one of the following ICMP type codes: <ul style="list-style-type: none"> <li>• 0—Echo reply</li> <li>• 8—Echo request</li> <li>• 3:[0-15]—Destination unreachable</li> <li>• 5:[0-3]—ICMP redirects</li> </ul> |

#### Examples of acceptable ACL Format:

permit tcp any host 192.168.1.100 eq 80—permits www traffic from anywhere to host 192.168.1.100

permit udp any eq 68 any eq 67—permits dhcp traffic

permit icmp any any 8, permit icmp any any 0—allows icmp echo-request and echo-reply

deny icmp any any 5:0—denies icmp network redirects

permit ip any 67.2.2.0 0.0.0.255 —permits all traffic from the host to 67.2.2.0 subnet

permit udp any any range 16384 32767—permits voice traffic using range of udp ports

#### Examples of incorrect syntax

permit ip 192.168.2.100 192.168.1.100—host/wildcard keyword missing

permit tcp host 192.168.2.100 host 192.168.1.100 eq 88 389 636 454 3268 3269 1025 1026 (You cannot club multiple ports using eq operator, and this ACL needs to be split into multiple lines one for each destination port)



#### Note

The source address for all ACEs must be defined as ANY.

## 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.



## Cisco ISE Endpoint Profiling Policies

---

- [Cisco ISE Profiling Service, page 469](#)
- [Configure Profiling Service in Cisco ISE Nodes, page 471](#)
- [Network Probes Used by Profiling Service, page 471](#)
- [Configure Probes per Cisco ISE Node, page 479](#)
- [Setup CoA, SNMP RO Community, and Endpoint Attribute Filter, page 480](#)
- [Attribute Filters for ISE Database Persistence and Performance, page 483](#)
- [Attributes Collection from IOS Sensor Embedded Switches, page 486](#)
- [Endpoint Profiling Policy Rules, page 487](#)
- [Create Endpoint Profiling Policies, page 488](#)
- [Predefined Endpoint Profiling Policies, page 491](#)
- [Endpoint Profiling Policies Grouped into Logical Profiles, page 494](#)
- [Profiling Exception Actions, page 495](#)
- [Profiling Network Scan Actions, page 495](#)
- [Cisco ISE Integration with Cisco NAC Appliance, page 503](#)
- [Create Endpoints with Static Assignments of Policies and Identity Groups, page 504](#)
- [Identified Endpoints, page 509](#)
- [Create Endpoint Identity Groups, page 511](#)
- [Profiler Feed Service, page 513](#)
- [Profiler Reports, page 516](#)

### 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.

## 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.
- **Event Handler**—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.
- 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.

**Table 22: DHCP Client Messages from Different States**

| —                 | INIT-REBOOT | SELECTING | RENEWING   | REBINDING  |
|-------------------|-------------|-----------|------------|------------|
| broadcast/unicast | broadcast   | broadcast | unicast    | broadcast  |
| server-ip         | MUST NOT    | MUST      | MUST NOT   | MUST NOT   |
| requested-ip      | MUST        | MUST      | MUST NOT   | MUST NOT   |
| ciaddr            | zero        | zero      | IP address | IP address |

## 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 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 from Reject (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.

You can also run a manual subnet scan from the same location that you enable NMAP in the Admin console.

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 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 **Administration > Identities > Latest Network 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/CSCOcprm/logs/nmapSubnet.log
--append-output -oX - <subnet>
```

**Table 23: NMAP Commands for a Manual Subnet Scan**

|                  |                                                     |
|------------------|-----------------------------------------------------|
| -O               | Enables OS detection                                |
| -sU              | UDP scan                                            |
| -p <port ranges> | Scans only specified ports. For example, U:161, 162 |
| oN               | Normal output                                       |
| oX               | XML output                                          |

### 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 “ifPhysAddress”. 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**.

## Latest Network Scan Results

The most recent network scan results are stored in Administration > Identity Management > Identities > Latest Network Scan Results.

The Latest Network Scan Results Endpoints 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.

## 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

## DNS Lookup with an Inline Posture Node Deployment in Bridged Mode

For the Domain Name Service probe to work with Inline Posture deployment in the Bridged mode, you must configure the callStationIdType information sent in RADIUS messages for the Wireless LAN Controllers (WLCs). The Framed-IP-Address attribute in RADIUS messages does not contain the Call Station ID type in the MAC address format. Therefore RADIUS messages cannot be associated with the MAC address of endpoints, and the DNS probe is unable to perform the reverse DNS lookup. In order to profile endpoints, you must enable the RADIUS, and DNS probes in Cisco ISE, and then configure the WLCs to send the calling station ID in the MAC address format instead of the current IP address format in RADIUS messages. The WLCs must be configured to send the calling station ID in the MAC address format instead of the current IP address format in RADIUS messages. Once the callStationIdType is configured in the WLCs, the configuration uses the selected calling station ID for communications with RADIUS servers and other applications. It results in endpoints authentication, and then the DNS probe does a reverse DNS lookup (FQDN lookup) against the specified name servers and update the FQDN of endpoints.

## 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 Delimiter 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 `cdp run` command on a network device, and enable the Cisco Discovery Protocol by using the `cdp enable` 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 24: Default LLDP Configuration**

| Feature                              | Feature                               |
|--------------------------------------|---------------------------------------|
| LLDP global state                    | Disabled                              |
| LLDP holdtime (before discarding)    | 120 seconds                           |
| LLDP timer (packet update frequency) | 30 seconds                            |
| LLDP reinitialization delay          | 2 seconds                             |
| LLDP tlv-select                      | Enabled to send and receive all TLVs. |
| LLDP interface state                 | Enabled                               |
| LLDP receive                         | Enabled                               |
| LLDP transmit                        | Enabled                               |
| LLDP med-tlv-select                  | Enabled to send all LLDP-MED TLVs     |

### 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.

**Note**


---

Cisco ISE does not support SNMP Traps that are received from the Wireless LAN Controllers (WLCs) and Access Points (APs).

---

**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.
- Multiple nodes—If you have registered more than one node in your deployment that assume Policy Service persona.

### 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.

- Step 3** Enter new SNMP community strings separated by a comma for the NMAP manual network scan in the **Change custom SNMP community strings** field, and re-enter the strings in the **Confirm custom SNMP community strings** field for confirmation.
- Step 4** Check the **Endpoint Attribute Filter** check box to enable endpoint attribute filtering.
- Step 5** Click **Save**.
- 

## 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 25: Change of Authorization Issued for Each Type of CoA Configuration**

| Scenarios                                                     | No CoA Configuration | Port Bounce Configuration                    | Reauth Configuration | Additional Information                                                                      |
|---------------------------------------------------------------|----------------------|----------------------------------------------|----------------------|---------------------------------------------------------------------------------------------|
| Global CoA configuration in Cisco ISE (typical configuration) | No CoA               | Port Bounce                                  | Reauthentication     | —                                                                                           |
| An endpoint is disconnected on your network                   | No CoA               | No CoA                                       | No CoA               | Change of authorization is determined by the RADIUS attribute Acct-Status -Type value Stop. |
| Wired with multiple active sessions on the same switch port   | No CoA               | Reauthentication                             | Reauthentication     | Reauthentication avoids disconnecting other sessions.                                       |
| Wireless endpoint                                             | No CoA               | Packet-of-Disconnect CoA (Terminate Session) | Reauthentication     | Support to Wireless LAN Controller.                                                         |
| Incomplete CoA data                                           | No CoA               | No CoA                                       | No CoA               | Due to missing RADIUS attributes.                                                           |

## 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 white list 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 26: Whitelist Attributes**

|                           |                             |
|---------------------------|-----------------------------|
| AAA-Server                | BYODRegistration            |
| Calling-Station-ID        | Certificate Expiration Date |
| Certificate Issue Date    | Certificate Issuer Name     |
| Certificate Serial Number | Description                 |
| DestinationIPAddress      | Device Identifier           |
| Device Name               | DeviceRegistrationStatus    |
| EndPointPolicy            | EndPointPolicyID            |
| EndPointProfilerServer    | EndPointSource              |
| FQDN                      | FirstCollection             |

|                              |                        |
|------------------------------|------------------------|
| Framed-IP-Address            | IdentityGroup          |
| IdentityGroupID              | IdentityStoreGUID      |
| IdentityStoreName            | L4_DST_PORT            |
| LastNmapScanTime             | MACAddress             |
| MatchedPolicy                | MatchedPolicyID        |
| NADAddress                   | NAS-IP-Address         |
| NAS-Port-Id                  | NAS-Port-Type          |
| NmapScanCount                | NmapSubnetScanID       |
| OS Version                   | OUI                    |
| PolicyVersion                | PortalUser             |
| PostureApplicable            | Product                |
| RegistrationTimeStamp        | —                      |
| StaticAssignment             | StaticGroupAssignment  |
| TimeToProfile                | Total Certainty Factor |
| User-Agent                   | cdpCacheAddress        |
| cdpCacheCapabilities         | cdpCacheDeviceId       |
| cdpCachePlatform             | cdpCacheVersion        |
| ciaddr                       | dhcp-class-identifier  |
| dhcp-requested-address       | host-name              |
| hrDeviceDescr                | ifIndex                |
| ip                           | lldpCacheCapabilities  |
| lldpCapabilitiesMapSupported | lldpSystemDescription  |
| operating-system             | sysDescr               |
| 161-udp                      | —                      |

## 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**.

### 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.

---

## 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.

**Note**

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 27: CoA Type Issued for Various Combination of Configuration**

| Global CoA Type | Default CoA Type set per Policy | No coA Type per Policy | Port Bounce Type per Policy | Reauth Type per Policy |
|-----------------|---------------------------------|------------------------|-----------------------------|------------------------|
| No CoA          | No CoA                          | No CoA                 | No CoA                      | No CoA                 |
| Port Bounce     | Port Bounce                     | No CoA                 | Port Bounce                 | Re-Auth                |
| Reauth          | Reauth                          | No CoA                 | Port Bounce                 | Re-Auth                |

## 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.

---

**Step 1** Choose **Policy > Profiling > Profiling > Profiling Policies**.

**Step 2** Choose **Export**, and choose one of the following:

- **Export Selected**—You can export only the selected endpoint profiling policies in the Profiling Policies page.
- **Export Selected with Endpoints**—You can export the selected endpoint profiling policies, and the endpoints that are profiled with the selected endpoint profiling policies.
- **Export All**—By default, you can export all the profiling policies in the Profiling Policies page.

**Step 3** Click **OK to export the endpoint profiling policies** in the profiler\_policies.xml file.

---

## 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
- Draeger-M300PortCheck3 that contains port 2150

## 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 494.

- 
- 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 can not 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**.
- 

## 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**.
- 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.
- 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 28: NMAP Commands for a Manual Subnet Scan**

|                  |                                                     |
|------------------|-----------------------------------------------------|
| -O               | Enables OS detection                                |
| -sU              | UDP scan                                            |
| -p <port ranges> | Scans only specified ports. For example, U:161, 162 |
| oN               | Normal output                                       |
| oX               | XML output                                          |

## 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.

|     |     |     |     |     |     |     |     |     |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 1   | 3   | 4   | 6   | 7   | 9   | 13  | 17  | 19  |
| 20  | 21  | 22  | 23  | 24  | 25  | 26  | 30  | 32  |
| 33  | 37  | 42  | 43  | 49  | 53  | 70  | 79  | 80  |
| 81  | 82  | 83  | 84  | 85  | 88  | 89  | 90  | 99  |
| 100 | 106 | 109 | 110 | 111 | 113 | 119 | 125 | 135 |
| 139 | 143 | 144 | 146 | 161 | 163 | 179 | 199 | 211 |
| 212 | 222 | 254 | 255 | 256 | 259 | 264 | 280 | 301 |
| 306 | 311 | 340 | 366 | 389 | 406 | 407 | 416 | 417 |
| 425 | 427 | 443 | 444 | 445 | 458 | 464 | 465 | 481 |
| 497 | 500 | 512 | 513 | 514 | 515 | 524 | 541 | 543 |
| 544 | 545 | 548 | 554 | 555 | 563 | 587 | 593 | 616 |

|      |      |      |      |           |           |           |           |           |
|------|------|------|------|-----------|-----------|-----------|-----------|-----------|
| 617  | 625  | 631  | 636  | 646       | 648       | 666       | 667       | 668       |
| 683  | 687  | 691  | 700  | 705       | 711       | 714       | 720       | 722       |
| 726  | 749  | 765  | 777  | 783       | 787       | 800       | 801       | 808       |
| 843  | 873  | 880  | 888  | 898       | 900       | 901       | 902       | 903       |
| 911  | 912  | 981  | 987  | 990       | 992       | 993       | 995       | 999       |
| 1000 | 1001 | 1002 | 1007 | 1009      | 1010      | 1011      | 1021      | 1022      |
| 1023 | 1024 | 1025 | 1026 | 1027      | 1028      | 1029      | 1030      | 1031      |
| 1032 | 1033 | 1034 | 1035 | 1036      | 1037      | 1038      | 1039      | 1040-1100 |
| 1102 | 1104 | 1105 | 1106 | 1107      | 1108      | 1110      | 1111      | 1112      |
| 1113 | 1114 | 1117 | 1119 | 1121      | 1122      | 1123      | 1124      | 1126      |
| 1130 | 1131 | 1132 | 1137 | 1138      | 1141      | 1145      | 1147      | 1148      |
| 1149 | 1151 | 1152 | 1154 | 1163      | 1164      | 1165      | 1166      | 1169      |
| 1174 | 1175 | 1183 | 1185 | 1186      | 1187      | 1192      | 1198      | 1199      |
| 1201 | 1213 | 1216 | 1217 | 1218      | 1233      | 1234      | 1236      | 1244      |
| 1247 | 1248 | 1259 | 1271 | 1272      | 1277      | 1287      | 1296      | 1300      |
| 1301 | 1309 | 1310 | 1311 | 1322      | 1328      | 1334      | 1352      | 1417      |
| 1433 | 1434 | 1443 | 1455 | 1461      | 1494      | 1500      | 1501      | 1503      |
| 1521 | 1524 | 1533 | 1556 | 1580      | 1583      | 1594      | 1600      | 1641      |
| 1658 | 1666 | 1687 | 1688 | 1700      | 1717      | 1718      | 1719      | 1720      |
| 1721 | 1723 | 1755 | 1761 | 1782      | 1783      | 1801      | 1805      | 1812      |
| 1839 | 1840 | 1862 | 1863 | 1864      | 1875      | 1900      | 1914      | 1935      |
| 1947 | 1971 | 1972 | 1974 | 1984      | 1998-2010 | 2013      | 2020      | 2021      |
| 2022 | 2030 | 2033 | 2034 | 2035      | 2038      | 2040-2043 | 2045-2049 | 2065      |
| 2068 | 2099 | 2100 | 2103 | 2105-2107 | 2111      | 2119      | 2121      | 2126      |
| 2135 | 2144 | 2160 | 2161 | 2170      | 2179      | 2190      | 2191      | 2196      |



|           |           |           |      |      |      |           |      |           |
|-----------|-----------|-----------|------|------|------|-----------|------|-----------|
| 2200      | 2222      | 2251      | 2260 | 2288 | 2301 | 2323      | 2366 | 2381-2383 |
| 2393      | 2394      | 2399      | 2401 | 2492 | 2500 | 2522      | 2525 | 2557      |
| 2601      | 2602      | 2604      | 2605 | 2607 | 2608 | 2638      | 2701 | 2702      |
| 2710      | 2717      | 2718      | 2725 | 2800 | 2809 | 2811      | 2869 | 2875      |
| 2909      | 2910      | 2920      | 2967 | 2968 | 2998 | 3000      | 3001 | 3003      |
| 3005      | 3006      | 3007      | 3011 | 3013 | 3017 | 3030      | 3031 | 3052      |
| 3071      | 3077      | 3128      | 3168 | 3211 | 3221 | 3260      | 3261 | 3268      |
| 3269      | 3283      | 3300      | 3301 | 3306 | 3322 | 3323      | 3324 | 3325      |
| 3333      | 3351      | 3367      | 3369 | 3370 | 3371 | 3372      | 3389 | 3390      |
| 3404      | 3476      | 3493      | 3517 | 3527 | 3546 | 3551      | 3580 | 3659      |
| 3689      | 3690      | 3703      | 3737 | 3766 | 3784 | 3800      | 3801 | 3809      |
| 3814      | 3826      | 3827      | 3828 | 3851 | 3869 | 3871      | 3878 | 3880      |
| 3889      | 3905      | 3914      | 3918 | 3920 | 3945 | 3971      | 3986 | 3995      |
| 3998      | 4000-4006 | 4045      | 4111 | 4125 | 4126 | 4129      | 4224 | 4242      |
| 4279      | 4321      | 4343      | 4443 | 4444 | 4445 | 4446      | 4449 | 4550      |
| 4567      | 4662      | 4848      | 4899 | 4900 | 4998 | 5000-5004 | 5009 | 5030      |
| 5033      | 5050      | 5051      | 5054 | 5060 | 5061 | 5080      | 5087 | 5100      |
| 5101      | 5102      | 5120      | 5190 | 5200 | 5214 | 5221      | 5222 | 5225      |
| 5226      | 5269      | 5280      | 5298 | 5357 | 5405 | 5414      | 5431 | 5432      |
| 5440      | 5500      | 5510      | 5544 | 5550 | 5555 | 5560      | 5566 | 5631      |
| 5633      | 5666      | 5678      | 5679 | 5718 | 5730 | 5800      | 5801 | 5802      |
| 5810      | 5811      | 5815      | 5822 | 5825 | 5850 | 5859      | 5862 | 5877      |
| 5900-5907 | 5910      | 5911      | 5915 | 5922 | 5925 | 5950      | 5952 | 5959      |
| 5960-5963 | 5987-5989 | 5998-6007 | 6009 | 6025 | 6059 | 6100      | 6101 | 6106      |
| 6112      | 6123      | 6129      | 6156 | 6346 | 6389 | 6502      | 6510 | 6543      |

|           |           |       |       |       |       |       |       |       |
|-----------|-----------|-------|-------|-------|-------|-------|-------|-------|
| 6547      | 6565-6567 | 6580  | 6646  | 6666  | 6667  | 6668  | 6669  | 6689  |
| 6692      | 6699      | 6779  | 6788  | 6789  | 6792  | 6839  | 6881  | 6901  |
| 6969      | 7000      | 7001  | 7002  | 7004  | 7007  | 7019  | 7025  | 7070  |
| 7100      | 7103      | 7106  | 7200  | 7201  | 7402  | 7435  | 7443  | 7496  |
| 7512      | 7625      | 7627  | 7676  | 7741  | 7777  | 7778  | 7800  | 7911  |
| 7920      | 7921      | 7937  | 7938  | 7999  | 8000  | 8001  | 8002  | 8007  |
| 8008      | 8009      | 8010  | 8011  | 8021  | 8022  | 8031  | 8042  | 8045  |
| 8080-8090 | 8093      | 8099  | 8100  | 8180  | 8181  | 8192  | 8193  | 8194  |
| 8200      | 8222      | 8254  | 8290  | 8291  | 8292  | 8300  | 8333  | 8383  |
| 8400      | 8402      | 8443  | 8500  | 8600  | 8649  | 8651  | 8652  | 8654  |
| 8701      | 8800      | 8873  | 8888  | 8899  | 8994  | 9000  | 9001  | 9002  |
| 9003      | 9009      | 9010  | 9011  | 9040  | 9050  | 9071  | 9080  | 9081  |
| 9090      | 9091      | 9099  | 9100  | 9101  | 9102  | 9103  | 9110  | 9111  |
| 9200      | 9207      | 9220  | 9290  | 9415  | 9418  | 9485  | 9500  | 9502  |
| 9503      | 9535      | 9575  | 9593  | 9594  | 9595  | 9618  | 9666  | 9876  |
| 9877      | 9878      | 9898  | 9900  | 9917  | 9929  | 9943  | 9944  | 9968  |
| 9998      | 9999      | 10000 | 10001 | 10002 | 10003 | 10004 | 10009 | 10010 |
| 10012     | 10024     | 10025 | 10082 | 10180 | 10215 | 10243 | 10566 | 10616 |
| 10617     | 10621     | 10626 | 10628 | 10629 | 10778 | 11110 | 11111 | 11967 |
| 12000     | 12174     | 12265 | 12345 | 13456 | 13722 | 13782 | 13783 | 14000 |
| 14238     | 14441     | 14442 | 15000 | 15002 | 15003 | 15004 | 15660 | 15742 |
| 16000     | 16001     | 16012 | 16016 | 16018 | 16080 | 16113 | 16992 | 16993 |
| 17877     | 17988     | 18040 | 18101 | 18988 | 19101 | 19283 | 19315 | 19350 |
| 19780     | 19801     | 19842 | 20000 | 20005 | 20031 | 20221 | 20222 | 20828 |
| 21571     | 22939     | 23502 | 24444 | 24800 | 25734 | 25735 | 26214 | 27000 |

|       |       |       |       |       |       |       |       |       |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|
| 27352 | 27353 | 27355 | 27356 | 27715 | 28201 | 30000 | 30718 | 30951 |
| 31038 | 31337 | 32768 | 32769 | 32770 | 32771 | 32772 | 32773 | 32774 |
| 32775 | 32776 | 32777 | 32778 | 32779 | 32780 | 32781 | 32782 | 32783 |
| 32784 | 32785 | 33354 | 33899 | 34571 | 34572 | 34573 | 34601 | 35500 |
| 36869 | 38292 | 40193 | 40911 | 41511 | 42510 | 44176 | 44442 | 44443 |
| 44501 | 45100 | 48080 | 49152 | 49153 | 49154 | 49155 | 49156 | 49157 |
| 49158 | 49159 | 49160 | 49161 | 49163 | 49165 | 49167 | 49175 | 49176 |
| 49400 | 49999 | 50000 | 50001 | 50002 | 50003 | 50006 | 50300 | 50389 |
| 50500 | 50636 | 50800 | 51103 | 51493 | 52673 | 52822 | 52848 | 52869 |
| 54045 | 54328 | 55055 | 55056 | 55555 | 55600 | 56737 | 56738 | 57294 |
| 57797 | 58080 | 60020 | 60443 | 61532 | 61900 | 62078 | 63331 | 64623 |
| 64680 | 65000 | 65129 | 65389 |       |       |       |       |       |

## 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 -p U:161,162 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP-address>
```

**Table 29: NMAP Commands for an Endpoint SNMP Port Scan**

|                  |                                                                       |
|------------------|-----------------------------------------------------------------------|
| -sU              | UDP scan.                                                             |
| -p <port-ranges> | Scans only specified ports. For example, scans UDP ports 161 and 162. |
| oN               | Normal output.                                                        |
| oX               | XML output.                                                           |
| IP-address       | IP-address of an endpoint that is scanned.                            |

## 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: `nmap -sTU -p T:21,22,23,25,53,80,110,135,139,143,443,445,3306,3389,8080,U:53,67,68,123,135,137,138,139,161,445,500,520,631,1434,1900 -oN /opt/CSCOcpm/logs/nmap.log --append-output -oX - <IP address>`

**Table 30: NMAP Commands for an Endpoint Common Ports Scan**

|                  |                                                                                                                                                       |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| -sTU             | Both TCP connect scan and UDP scan.                                                                                                                   |
| -p <port ranges> | Scans TCP ports: 21,22,23,25,53,80,110,135,139,143, 443,445,3306,3389,8080 and UDP ports: 53,67,68,123,135,137, 138,139,161,445,500,520,631,1434,1900 |
| oN               | Normal output.                                                                                                                                        |
| oX               | XML output.                                                                                                                                           |
| IP address       | IP address of an endpoint that is scanned.                                                                                                            |

## Common Ports

The following table lists the common ports that NMAP uses for scanning.

**Table 31: Common Ports**

| TCP Ports |              | UDP Ports |              |
|-----------|--------------|-----------|--------------|
| Ports     | Service      | Ports     | Service      |
| 21/tcp    | ftp          | 53/udp    | domain       |
| 22/tcp    | ssh          | 67/udp    | dhcps        |
| 23/tcp    | telnet       | 68/udp    | dhcpc        |
| 25/tcp    | smtp         | 123/udp   | ntp          |
| 53/tcp    | domain       | 135/udp   | msrpc        |
| 80/tcp    | http         | 137/udp   | netbios-ns   |
| 110/tcp   | pop3         | 138/udp   | netbios-dgm  |
| 135/tcp   | msrpc        | 139/udp   | netbios-ssn  |
| 139/tcp   | netbios-ssn  | 161/udp   | snmp         |
| 143/tcp   | imap         | 445/udp   | microsoft-ds |
| 443/tcp   | https        | 500/udp   | isakmp       |
| 445/tcp   | microsoft-ds | 520/udp   | route        |
| 3389/tcp  | ms-term-serv | 1434/udp  | ms-sql-m     |

| TCP Ports |            | UDP Ports |         |
|-----------|------------|-----------|---------|
| Ports     | Service    | Ports     | Service |
| 8080/tcp  | http-proxy | 1900/udp  | upnp    |

## 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 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 PAN is responsible for all the communication between Cisco ISE and the Cisco NAC Appliance. You can configure CAMs only in the PAN in Cisco ISE. The credentials that are used at the time of registering one or more CAMs in the 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 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 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:

- Configuration changes for NAC Settings (Information)
- NAC notification event failure (Error)

## 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**.
- 

## 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 **Administration > Identity Management > 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 for which you have already exported endpoints from a Cisco ISE server, or a CSV file that you have created from Cisco ISE and updated with endpoint details.

The file format has to be in the format as specified in the default import template so that the list of endpoints appears as follows: MAC, Endpoint Policy, Endpoint Identity Group.

Both endpoint policy and endpoint identity group are optional for importing endpoints in a CSV file. If you want to import the endpoint identity group without the endpoint policy for endpoints, the values are still separated by the comma.

For example,

- MAC1, Endpoint Policy1, Endpoint Identity Group1
- MAC2
- MAC3, Endpoint Policy3

- MAC4, , Endpoint Identity Group4

- 
- Step 1** Choose **Administration > Identity Management > Identities > Endpoints > Import**.
- Step 2** Click **Import From File**.
- Step 3** Click Browse to locate the CSV file that you have already exported from the Cisco ISE server or the CSV file that you have created and updated with endpoints in the file format as specified.
- 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 **Administration > Identity Management > Identities > 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, columns.

You must update the MAC addresses of endpoints, endpoint profiling policies, and endpoint identity groups and save the file with a different file name that you can use to import endpoints. See the header row in the template.csv file that is created when you use the Generate a Template link.

**Table 32: CSV Template File**

| MAC               | Endpoint Policy | Endpoint Identity Group |
|-------------------|-----------------|-------------------------|
| 00:1f:f3:4e:c1:8e | Cisco-Device    | RegisteredDevices       |

### 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 33: Unknown Profiles: Import from a File**

| MAC Address       | Endpoint Profiling Policy Assigned Before Import in Cisco ISE                                                                      | Endpoint Profiling Policy Assigned After Import in Cisco ISE |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| 00:00:00:00:01:02 | Unknown.                                                                                                                           | Xerox-Device                                                 |
| 00:00:00:00:01:03 | Unknown.                                                                                                                           | Xerox-Device                                                 |
| 00:00:00:00:01:04 | Unknown.                                                                                                                           | Xerox-Device                                                 |
| 00:00:00:00:01:05 | If no profile is assigned to an endpoint, then it is assigned to the Unknown profile, and also reprofiled to the matching profile. | Xerox-Device                                                 |

### Static Assignments of Policies and Identity Groups for Endpoints Retained During Import

If the file used for import contains endpoints that have their MAC addresses, and their assigned endpoint profiling policy is the static assignment, then they are not reprofiled during import. See below how Cisco ISE retains the Cisco-Device profile, the static assignment of an endpoint during import.

**Table 34: Static Assignment: Import From a File**

| MAC Address       | Endpoint Profiling Policy Assigned Before Import in Cisco ISE | Endpoint Profiling Policy Assigned After Import in Cisco ISE |
|-------------------|---------------------------------------------------------------|--------------------------------------------------------------|
| 00:00:00:00:01:02 | Cisco-Device (static assignment)                              | Cisco-Device                                                 |

### 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 35: Invalid Profiles: Import from a File**

| MAC Address       | Endpoint Profiling Policy Assigned Before Import in Cisco ISE                                                                                                                                                                                        | Endpoint Profiling Policy Assigned After Import in Cisco ISE                    |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| 00:00:00:00:01:02 | Unknown.                                                                                                                                                                                                                                             | Xerox-Device                                                                    |
| 00:00:00:00:01:05 | 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. | The endpoint is not imported because there is no matching profile in Cisco ISE. |

## 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 **Administration > Identity Management > Identities > 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 to different Cisco ISE servers in a comma-separated values (CSV) file in which endpoints are listed with their MAC addresses, endpoint profiling policies, and endpoint identity groups to which they are assigned.

Export All is the default option. If endpoints are filtered in the Endpoints page, only those filtered endpoints are exported when you are using the Export All option. By default, the profiler\_endpoints.csv is the CSV file and the Microsoft Office Excel is the default application to open the CSV file from the Opening profiler\_endpoints.csv dialog box or to save the CSV file. For example, you can export selected endpoints or all endpoints in the profiler\_endpoints.csv file, which you can use to import those endpoints.

- 
- Step 1** Choose **Administration > Identity Management > Identities > 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 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.

- 
- 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 > Authorization > Standard**.

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.

By default, the profiler feed service is disabled, and it requires a Plus license to enable the service. When you enable the profiler feed service, 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.

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.

## 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**).

- 
- 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 **Administration > FeedService > Profiler**.
- Step 3** 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 4** Check the **Enable Profiler Feed Service** check box.
- Step 5** Enter time in HH:MM format (local time zone of the Cisco ISE server) in the Feed Service Scheduler section. By default, Cisco ISE feed service is scheduled at 1.00 AM every day.
- Step 6** Check the **Notify administrator when download occurs** check box in the Administrator Notification Options section and enter your e-mail address as an administrator of Cisco ISE in the **Administrator email address** text box.
- Step 7** Check the **Provide subscriber information to Cisco** check box in the Feed Service Subscriber Information section and enter your details as an administrator of Cisco ISE and an alternate Cisco ISE administrator details.
- Step 8** Click **Accept**.
- Step 9** Click **Save**.
- Step 10** 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.
- Step 11** Click **Yes**.
- 

## Remove Updates to Endpoint Profiling Policies

You can revert endpoint profiling policies that were updated in the previous update and remove endpoint profiling policies that are newly added through the previous update of the profiler feed service but OUI updates are not changed.

An endpoint profiling policy, if modified after an update from the feed server is not changed in the system.

- 
- Step 1** Choose **Administration > FeedService > Profiler**.
- Step 2** Check the **Enable Profiler Feed Service** check box.
- Step 3** Click **Go to Update Report Page** if you want to view the configuration changes made in the Change Configuration Audit report.
- Step 4** 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



## Configure Client Provisioning

---

- [Enable Client Provisioning in Cisco ISE, page 518](#)
- [Client Provisioning Resources, page 518](#)
- [Add Client Provisioning Resources from Cisco, page 519](#)
- [Download Client Provisioning Resources Automatically, page 519](#)
- [Add Cisco Provided Client Provisioning Resources from a Local Machine, page 520](#)
- [Add Customer Created Resources for AnyConnect from a Local Machine, page 521](#)
- [Configure Personal Device Registration Behavior, page 522](#)
- [Create Native Supplicant Profiles, page 522](#)
- [AMP Enabler Profile Settings, page 524](#)
- [Create AnyConnect Configuration, page 527](#)
- [Create AnyConnect and Cisco NAC Agent Profiles, page 528](#)
- [Agent Profile Configuration Guidelines, page 529](#)
- [Client IP Address Refresh Configuration, page 535](#)
- [Posture Protocol Settings, page 540](#)
- [Client Login Session Criteria, page 543](#)
- [Provision Client Machines with the Cisco NAC Agent MSI Installer, page 544](#)
- [Cisco ISE Posture Agents, page 545](#)
- [AnyConnect, page 546](#)
- [Cisco NAC Agent XML File Installation Directories, page 547](#)
- [Cisco NAC Agent for Windows Clients, page 547](#)
- [Cisco NAC Agent for Macintosh Clients, page 549](#)
- [Cisco Web Agent, page 549](#)
- [Cisco NAC Agent Logs, page 550](#)
- [Create an Agent Customization File for the Cisco NAC Agent, page 550](#)

- [Configure Client Provisioning Resource Policies](#), page 561
- [Client Provisioning Reports](#), page 564
- [Client Provisioning Event Logs](#), page 564

## Enable Client Provisioning in Cisco ISE

Client provisioning functions in Cisco ISE allow you to download client provisioning resources and configure agent profiles for Windows and MAC OS X clients, and native supplicant profiles for your own personal devices. Client provisioning resource policies enable users to download and install resources on client devices.

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. When you choose to disable this function of Cisco ISE, users who attempt to access the network will receive a warning message indicating that they are not able to download client provisioning resources.

### Before You Begin

To ensure that you are able to access the appropriate remote location from which you can download client provisioning resources to Cisco ISE, you may be required to verify that you have the correct proxy settings configured for your network.

- 
- Step 1** Choose **Administration > System > Settings > Client Provisioning**.
- Step 2** From the Enable Provisioning drop-down list, choose **Enable** or **Disable**.
- Step 3** Click **Save**.
- 

### What to Do Next

Add client provisioning resources for posture agents in Cisco ISE and configure client provisioning policies to enable users to download and install client provisioning resources on client machines.

## 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 [Download Client Provisioning Resources Automatically](#).

- **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 520](#).
- **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, see [AnyConnect Administrators Guide, ISE Posture Profile Editor](#). For more information about the NAC agent profile, see [Create an Agent Customization File for the Cisco NAC Agent, on page 550](#).

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 561](#).

## 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.

## Download Client Provisioning Resources Automatically

Downloading automatically uploads all available software from Cisco to Cisco ISE, many items of which may not be pertinent to your deployment. Cisco recommends manually uploading resources whenever possible rather than opting to download them automatically from Cisco.

**Before You Begin**

Ensure that you have the correct proxy settings configured in Cisco ISE and you are able to access the appropriate remote location from which you can download client provisioning resources to Cisco ISE.

- 
- Step 1** Choose **Administration > System > Settings > Client Provisioning**.
- Step 2** From the **Enable Automatic Download** drop-down list, choose **Enable**.
- Step 3** 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-redirectation 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 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

## Configure Personal Device Registration Behavior

Use this function to specify how Cisco ISE should handle user login sessions via personal devices on which Cisco ISE cannot install a native supplicant provisioning wizard (For example, Research In Motion Blackberry devices).

- 
- Step 1** Choose **Administration > System > Settings > Client Provisioning**.
- Step 2** From the Native Supplicant Provisioning Policy Unavailable drop-down list, choose one of the following two options:
- 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 3** Click **Save**.
- 

### 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.

## 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 523
- 

### 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.
- **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.

- **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.

## 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 36: AMP Enabler Profile Page**

| Fields                | Usage Guidelines                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                  | Enter the name of the AMP enabler profile that you want to create.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Description           | Enter a description for the AMP enabler profile.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Install AMP Enabler   | <ul style="list-style-type: none"> <li>• <b>Windows Installer</b>—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.</li> <li>• <b>Mac Installer</b>—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.</li> </ul> <p>The <b>Check</b> 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.</p> |
| Uninstall AMP Enabler | Uninstalls the AMP for endpoint software from the endpoint.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

| Fields              | Usage Guidelines                                                                                                                                       |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.            |

## 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. You 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 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>
 <StartMenu>true</StartMenu>
 <DesktopIcon>false</DesktopIcon>
 <ContextIcon>true</ContextIcon>
 </Install>
 </FAConfiguration>
</FAProfile>
```

The following example shows a customized uninstall file.

```
<?xml version="1.0" encoding="UTF-8"?>
<FAProfile xsi:noNamespaceSchemaLocation="FAProfile.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <FAConfiguration>
 <Uninstall>
 </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 in to the Cisco ISE certificate store. Obtain a SOURCEfire trusted certificate and import it in to 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.

## 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.

### 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. VPNDisable\_ServiceProfile.xml is on CCO with the other AnyConnect files.
- 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.
- Step 10** Click **Submit**.
- 

## Create AnyConnect and Cisco NAC Agent Profiles

Use this procedure to create an AnyConnect or a NAC posture agent profile where you can specify parameters that define the agent behavior, parameters that are related to whether or not to refresh the client IP address, and 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** Choose **AnyConnect** or **NAC Agent**.
- Step 5** Configure parameters for the following:
- Cisco ISE posture agent behavior
  - Client IP Address Changes
  - Cisco ISE posture protocol

**Step 6** Click **Submit**.

## Agent Profile Configuration Guidelines

Cisco recommends configuring agent profiles to control remediation timers, network transition delay timers, and the timer that is used to automatically close the login success screen on client machines so that these settings are policy based. However, when there are no agent profiles configured to match client provisioning policies, you can use the settings in the **Administration > System > Settings > Posture > General Settings** to accomplish the same goal.

Once you configure and upload an agent profile to a client device via policy enforcement or another method, that agent profile remains on the client and affects login and operation behavior until you change it to something else. Therefore, deleting an agent profile from Cisco ISE does not remove that behavior from previously affected clients. To alter the login and operational behavior, you must define a new agent profile that overwrites the values of existing agent profile parameters on the client and upload it via policy enforcement.

If Cisco ISE has a different agent profile than what is present on the client (which is determined using MD5 checksum), then Cisco ISE downloads the new agent profile to the client. If the agent customization file originating from Cisco ISE is different, Cisco ISE also downloads the new agent customization file to the client.

## Agent Behavior Configuration

The following table describes the fields in the NAC or AnyConnect Posture Profile page, which allows you to configure parameters for the posture agent (AnyConnect and Cisco NAC Agent). The navigation path for this page is **Policy > Policy Elements > Results > Client Provisioning > Resources > Add > NAC or AnyConnect Posture Profile**.

| Field                                                      | Default Value | Mode (Applies only to Cisco ISE NAC Agent ) | Usage Guidelines                                                                                    |
|------------------------------------------------------------|---------------|---------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Disable Agent Exit. (Not applicable for a Mac OS X client) | No            | Merge                                       | If the value is set to Yes, this setting prevents users from exiting the agent via the system tray. |

| Field                                                            | Default Value                                                     | Mode (Applies only to Cisco ISE NAC Agent ) | Usage Guidelines                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------|-------------------------------------------------------------------|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable Accessibility Mode (Not applicable for a Mac OS X client) | No—Agent does not interact with the Job Access with Speech (JAWS) | Merge                                       | <p>If the value is set to Yes, this setting enables compatibility with the JAWS screen reader.</p> <p>Users may experience a slight impact on performance when this feature is enabled. The agent still functions normally if this feature is enabled on a client machine that does not have the JAWS screen reader installed.</p> |
| Enable signature check(Not applicable for a Mac OS X client)     | No                                                                | Overwrite                                   | <p>If the value is set to Yes, this setting enables Windows to check the digital signature of the executables before launching the programs for remediation.</p>                                                                                                                                                                   |
| Bypass Summary Screen(Not applicable for a Mac OS X client)      | Yes                                                               | Merge                                       |                                                                                                                                                                                                                                                                                                                                    |



| Field                                                       | Default Value  | Mode (Applies only to Cisco ISE NAC Agent ) | Usage Guidelines                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------|----------------|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Locale(Not applicable for a Mac OS X client)                | Default        | Merge                                       | <p>The default setting enables the agent to use the locale settings from the client operating system.</p> <p>If this setting is either the ID, the abbreviated name, or the full name of a supported language, the agent automatically displays the appropriate localized text in the agent dialogs on the client machine.</p>            |
| Posture report filter(Not applicable for a Mac OS X client) | Display Failed | Merge                                       | <p>If the value is set to Display Failed, the client posture assessment report display only remediation errors when the user clicks Show Details in the agent dialog.</p> <p>If the value is set to Display All, the client posture assessment report displays all the results when the user clicks Show Details in the agent dialog.</p> |

| Field                    | Default Value | Mode (Applies only to Cisco ISE NAC Agent ) | Usage Guidelines                                                                                                                                                                                         |
|--------------------------|---------------|---------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Remediation timer        | 4             | Overwrite                                   | This setting specifies the time to remediate any failed posture assessment checks on the client machine before having to go through the entire login process again. The valid range is 1 to 300 minutes. |
| Network transition delay | 3             | Overwrite                                   | This setting specifies the time to wait for the network transition (IP address change) to occur before beginning the remediation timer countdown. The valid range is 2- 30 seconds.                      |

| Field                                              | Default Value | Mode (Applies only to Cisco ISE NAC Agent ) | Usage Guidelines                                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------|---------------|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log file size                                      | 5             | Merge                                       | <p>This setting specifies file size in megabytes for the agent log files on the client machine.</p> <p>If the log file size is set to zero, the agent does not record any login or operation information for the user session on the client machine.</p> <p>If the log file size is other than zero, the agent records login and session information up to the specified number of megabytes.</p> |
| Enable Auto Close. (Not applicable for AnyConnect) | No            | Overwrite                                   | <p>if this setting is set to Yes, this setting allows the agent login dialog to close automatically following the user authentication.</p>                                                                                                                                                                                                                                                        |

| Field                                            | Default Value | Mode (Applies only to Cisco ISE NAC Agent ) | Usage Guidelines                                                                                                                                                                  |
|--------------------------------------------------|---------------|---------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auto close timer (Not applicable for AnyConnect) | 0             | Overwrite                                   | This setting enables the agent login screen to wait for a specified period of time and close automatically following the user authentication. The valid range is 0 to 30 seconds. |



**Note** Merge parameter values with existing agent profile settings or overwrite them to appropriately configure agent behavior on Windows and Mac OS X clients.



**Note** Agent log files are stored in a directory on the client machine. After the first login session, two files reside in the directory: one backup file from the previous log in session, and one new file containing login and operation from the current session. If the log file for the current session grows beyond the specified file size, the first segment of agent login and operation information automatically becomes the backup file in the directory, and the agent continues to record the latest entries in the current session file.

## Supported Languages

**Table 37: Supported Languages**

| Language           | ID   | Abbreviated Name | Full Name             |
|--------------------|------|------------------|-----------------------|
| English US         | 1033 | en               | English               |
| Catalan            | 1027 | ca               | Catalan (Spain)       |
| ChineseSimplified  | 2052 | zh_cn            | Chinese (Simplified)  |
| ChineseTraditional | 1028 | zh_tw            | Chinese (Traditional) |
| Czech              | 1029 | cs               | Czech                 |
| Danish             | 1030 | da               | Danish                |
| Dutch              | 1043 | nl               | Dutch (Standard)      |

| Language        | ID   | Abbreviated Name | Full Name                 |
|-----------------|------|------------------|---------------------------|
| Finnish         | 1035 | fi               | Finnish                   |
| French          | 1036 | fr               | French                    |
| FrenchCanadian  | 3084 | fr-ca            | French-Canadian           |
| German          | 1031 | de               | German                    |
| Hungarian       | 1038 | hu               | Hungarian                 |
| Italian         | 1040 | it               | Italian                   |
| Japanese        | 1041 | ja               | Japanese                  |
| Korean          | 1042 | ko               | Korean (Extended Wansung) |
| Norwegian       | 1044 | no               | Norwegian                 |
| Polish          | 1045 | pl               | Polish                    |
| Portuguese      | 2070 | pt               | Portuguese                |
| Russian         | 1049 | ru               | Russian                   |
| SerbianLatin    | 2074 | sr               | Serbian (Latin)           |
| SerbianCyrillic | 3098 | src              | Serbian (Cyrillic)        |
| Spanish         | 1034 | es               | Spanish (Traditional)     |
| Swedish         | 1053 | sv               | Swedish                   |
| Turkish         | 1055 | tr               | Turkish                   |

## 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**.

| Field                   | Default Value | Mode (Applies only to Cisco NAC Agent) | Usage Guidelines |
|-------------------------|---------------|----------------------------------------|------------------|
| VLAN detection interval | 0, 5          | Merge                                  |                  |

| Field | Default Value | Mode (Applies only to Cisco NAC Agent) | Usage Guidelines                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------|---------------|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       |               |                                        | <p>This setting is the interval at which the agent check for the VLAN change.</p> <p>For the Windows NAC agent, the default value is 0. By default, the access to authentication VLAN change feature is disabled for Windows. The valid range is 0 to 5 seconds.</p> <p>For the Mac OS X agent, the default value is 5. By default, the access to authentication VLAN change feature is enabled with VlanDetectInteval as 5 seconds for Mac OS X. The valid range is 5 to 900 seconds.</p> <p>0 —Access to Authentication VLAN change feature is disabled.</p> <p>1 to 5—Agent sends an Internet Control Message Protocol (ICMP) or Address Resolution Protocol (ARP) query every 5 seconds.</p> <p>6 to 900—An ICMP or ARP query is sent</p> |

| Field                                                                   | Default Value                   | Mode (Applies only to Cisco NAC Agent) | Usage Guidelines                                                                                                                                                                                |
|-------------------------------------------------------------------------|---------------------------------|----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                         |                                 |                                        | every x seconds.                                                                                                                                                                                |
| Enable VLAN detection without UI (Not applicable for a Mac OS X client) | No                              | Merge                                  | This setting enables or disables VLAN detection even when the user is not logged in.<br>No—VLAN detect feature is disabled.<br>Yes—VLAN detect feature is enabled.                              |
| Retry detection count                                                   | 3                               | Merge                                  | 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. |
| Ping or ARP                                                             | 0<br>The valid range is 0 to 2. | Merge                                  | This setting specifies the method used for detecting the client IP address change.<br>0—Poll using ICMP<br>1—Poll using ARP<br>2—Poll using ICMP first, then (if ICMP fails) ARP                |



| Field                    | Default Value                            | Mode (Applies only to Cisco NAC Agent) | Usage Guidelines                                                                                                                                                                                          |
|--------------------------|------------------------------------------|----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum timeout for ping | 1<br>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<br>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<br>The valid range is 0 to 60 seconds. | Overwrite                              | The setting specifies that the client machine waits before releasing its current IP address.                                                                                                              |

**Note**

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 AnyConnect Profile page, which allows you to configure the posture protocol settings. The navigation path for this page is **Policy > Policy Elements > Results > Client Provisioning > Resources > Add > NAC Agent or AnyConnect Posture Profile**.

| Field                                                             | Value                                                                                                | Mode      | Usage Guidelines                                                                                                                                                                                                            |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Allow CRL Checks<br>(Not applicable for a Mac OS X client)        | Yes                                                                                                  | Overwrite | If the value is set to No, this setting turns off checking the certificate revocation list (CRL) during discovery and negotiation.                                                                                          |
| MAC Address Exemption List (Not applicable for a Mac OS X client) | Enter MAC addresses separated by a comma.<br>For example,<br>AA:BB:CC:DD:EE:FF,<br>11:22:33:44:55:66 | Merge     | If you specify one or more MAC addresses in this setting, the agent does not advertise those MAC addresses to Cisco ISE during login and authentication to help prevent sending unnecessary MAC addresses over the network. |
| Discovery Host (Not applicable for a Mac OS X client)             | Enter the IP address or the fully qualified domain name (FQDN)                                       | Overwrite | This setting specifies the Discovery Host address or resolvable domain name that the agent uses to connect to Cisco ISE in a Layer 3 deployment.                                                                            |
| Enable Discovery Host<br>(Not applicable for a Mac OS X client)   | Yes                                                                                                  | Overwrite | Yes—User can specify a custom value in the Discovery Host field in the agent Properties dialog box.<br><br>No—Ensure that the user cannot update the value in the Discovery Host field on the client machine.               |

| Field                                                             | Value                                                                                                                  | Mode  | Usage Guidelines                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Server Name Rules                                                 | Enter the fully qualified domain name (FQDN) of the Cisco ISE server that are separated by a comma.                    | Merge | This field consists of comma-separated names of associated Cisco ISE servers. The agent uses the names in this list to authorize Cisco ISE access points. If this list is empty, then authorization is not performed. If any of the names is not found, then an error is reported.                                                                   |
| Auto-generated MAC Address (Not applicable for a Mac OS X client) | —                                                                                                                      | Merge | This setting supports Evolution-Data Optimized connects on the client machine. If the client machine does not have an active network interface card, the agent creates a dummy MAC address for the system.                                                                                                                                           |
| SWISS Timeout (Not applicable for a Mac OS X client)              | 1—Agent performs SWISS discovery as designed and no additional UDP response packet delay time out value is introduced. | Merge | If the value is set to greater than one, the agent waits the additional number of seconds for a SWISS UDP discovery response packet from Cisco ISE before sending another discovery packet. The agent makes this action to ensure that the network latency is not delaying the response packet en route. (SWISS Timeout only for UDP SWISS Timeouts) |

| Field                                                         | Value                                                                       | Mode  | Usage Guidelines                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------|-----------------------------------------------------------------------------|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disable L3 SWISS delay (Not applicable for a Mac OS X client) | No                                                                          | Merge | If this setting is set to Yes, the agent disables the ability to increase the transmission interval for Layer 3 discovery packets. Therefore, the Layer 3 discovery packets repeatedly go out every 5 seconds, just like Layer 2 packets.                                                                                                                                                                                     |
| HTTP Discovery Timeout (Not applicable for a Mac OS X client) | 30 (Default for Windows clients)<br>The valid range is 3 seconds and above. | Merge | This setting specifies the HTTP discovery timeout for which the HTTPS discovery from the agent waits for the discovery response from Cisco ISE. If there is no response for the specified time, then the discovery process times out.<br><br>If the value is set to 0, then the default client machine operating system timeout settings are used.<br><br>If the value is set to 1 or 2, automatically the value is set to 3. |

| Field                                               | Value                                                                        | Mode  | Usage Guidelines                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------------|------------------------------------------------------------------------------|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HTTP Timeout (Not applicable for a Mac OS X client) | 120 (Default for Windows clients)<br>The valid range is 3 seconds and above. | Merge | This setting specifies the HTTP timeout for which the HTTP request from the agent waits for the response. If there is no response for the specified time, then the request times out, and the discovery process times out.<br><br>If the value is set to 0, then the default client machine operating system timeout settings are used.<br><br>If the value is set to 1 or 2, automatically the value is set to 3. |

## 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.

## Provision Client Machines with the Cisco NAC Agent MSI Installer

You can place the MSI installer in a directory or a zip version of the same installer on the client machine along with an Agent configuration XML file (named **NACAgentCFG.xml**) containing the appropriate Agent profile information required to coincide with your network.

- 
- Step 1** Download the **nacagentsetup-win.msi** or **nacagentsetup-win.zip** installer file from the Cisco Software Download site from <http://software.cisco.com/download/navigator.html> and navigate to **Security > Access Control and Policy > Cisco Identity Services Engine > Cisco Identity Services Engine Software > Release 1.x**.
- Step 2** Place the **nacagentsetup-win.msi** file in a specific directory on the client machine (for example, C:\temp\nacagentsetup-win.msi):
- If you are copying the MSI installer directly over to the client, place the **nacagentsetup-win.msi** file into a directory on the client machine from which you plan to install the Cisco NAC Agent.
  - If you are using the **nacagentsetup-win.zip** installer, extract the contents of the zip file into the directory on the client machine from which you plan to install the Cisco NAC Agent.
- Step 3** Place an Agent configuration XML file in the same directory as the Cisco NAC Agent MSI package. If you are not connected to Cisco ISE, you can copy the **NACAgentCFG.xml** file from a client that has already been successfully provisioned. The file is located at C:\Program Files\Cisco\Cisco NAC Agent\NACAgentCFG.xml.
- As long as the Agent configuration XML file exists in the same directory as the MSI installer package, the installation process automatically places the Agent configuration XML file in the appropriate Cisco NAC Agent application directory so that the agent can point to the correct Layer 3 network location when it is first launched.
- Step 4** Open a Command prompt on the client machine and enter the following to execute the installation:
- ```
msiexec.exe /i NACAgentSetup-win.msi /qn /l*v c:\temp\agent-install.log
```
- (The /qn qualifier installs the Cisco NAC Agent completely silently. The /l*v logs the installation session in verbose mode.)
- To uninstall the NAC Agent, you can execute the following command:
- ```
msiexec /x NACAgentSetup-win-<version>.msi /qn
```

Installing a new version of the Agent using MSI will uninstall the old version and install the new version using the above commands.

**Step 5**

If you are using Altiris/SMS to distribute the MSI installer, place the Agent customization files in a sub-directory named "brand" in the directory "%TEMP%/CCAA". When the Cisco NAC Agent is installed in the client, the customization is applied to the Agent. To remove the customization, send a plain MSI without the customization files.

## Cisco ISE Posture Agents

Agents are applications that reside on client machines logging into the Cisco ISE network. Agents can be persistent (like the AnyConnect, Cisco NAC Agent 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 NAC Web Agent), 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**

Currently Cisco NAC Agent and Cisco NAC Web Agent support Client Provisioning Portal and Native Supplicant Provisioning. Cisco NAC Web Agent supports Central Web Authentication flow (CWA), but Cisco NAC Agent does not support CWA.

### 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 Mac OS x), 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.

### 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-WEBAGENT=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 **Guest Access > Configure > 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.

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 NAC Agent XML File Installation Directories

In a system where the Cisco NAC Agent installed at the default location, you can find the following .xml files in the following directories:

- The nac\_login.xml file is available in the “C:\Program Files\Cisco\Cisco NAC Agent\UI\nac\_divs\login” directory.
- In the nacStrings\_xx.xml file, the “xx” indicates the locale. You can find a complete list of the files in the “C:\Program Files\Cisco\Cisco NAC Agent\UI\cues\_utility” directory.

If the agent is installed at a different location, then the files would be available at “<Agent Installed path>\Cisco\Cisco NAC Agent\UI\nac\_divs\login” and “<Agent Installed path>\Cisco\Cisco NAC Agent\cues\_utility”.

## Cisco NAC Agent for Windows Clients

The Cisco NAC Agent provides the posture assessment and remediation for client machines.

Users can download and install the Cisco NAC Agent (read-only client software), which can check the host registry, processes, applications, and services. The Cisco NAC Agent can be used to perform Windows updates or antivirus and antispyware definition updates, launch qualified remediation programs, distribute files uploaded to the Cisco ISE server, distribute website links to web sites for users to download files to fix their system, or simply distribute information and instructions.

Cisco strongly recommends that you ensure that the latest Windows hotfixes and patches are installed on Windows XP clients so that the Cisco NAC Agent can establish a secure and encrypted communication with Cisco ISE (via SSL over TCP).

### Uninstall the Cisco NAC Agent from Windows 7 and Earlier Clients

The Cisco NAC Agent installs to **C:\Program Files\Cisco\Cisco NAC Agent\** on the Windows client.

You can uninstall the agent in the following ways:

- By double-clicking the **Uninstall Cisco NAC Agent** desktop icon.
- By going to **Start Menu > Programs > Cisco Systems > Cisco Clean Access > Uninstall Cisco NAC Agent**
- By going to **Start Menu > Control Panel > Add or Remove Programs > Cisco NAC Agent** and uninstall the Cisco NAC Agent.

## Uninstall the Cisco NAC Agent in a Windows 8 Client

You can uninstall Cisco NAC Agent in a Windows 8 client in Metro mode.

- 
- Step 1** Switch to Metro Mode.
- Step 2** Right-Click **Cisco NAC Agent** tile.
- Step 3** Select **Un-Install** from the options available at the bottom of the screen.
- Step 4** The system automatically switches to Desktop mode and opens **Add/Remove** control panel.
- Step 5** In the **Add/Remove** control panel, perform one of the following:
- a) Double Click **Cisco NAC Agent** and click **Uninstall**.
  - b) Select **Cisco NAC Agent** and click **Uninstall**.
  - c) Right Click **Cisco NAC Agent** and select **Uninstall**.
- 

## Windows 8 Metro and Metro App Support —Toast Notifications

The Enable Toast Notification option is available on the Cisco NAC Agent Tray Icon that can send relevant notifications to users on Windows 8 clients .

In Cisco NAC Agent scenarios where the user does not get network access, like "Remediation Failed" or "Network Access expired", the Agent displays the following toast notification:Network not available, Click "OK" to continue.

To get more details, you can select the toast and you will be redirected to Desktop mode and the Cisco NAC agent dialog is displayed.

Toast Notification is displayed for all positive recommended actions that the user needs to perform to gain network access. The following are some examples:

- For Network Acceptance policy, toast will be displayed as: "Click Accept to gain network access"
- For Agent/Compliance Module Upgrade, toast will be displayed as: "Click OK to Upgrade/Update"
- In the "user logged out" event, when "Auto Close" option for Logoff is not enabled in Clean Access Manager (CAM), toast notification is provided. This toast enables the users to know that they have been logged out and that they need to login again to get network access.

## Cisco NAC Agent for Macintosh Clients

The Cisco NAC OS X Agent provides the posture assessment and remediation for Macintosh client machines.

Users can download and install the Cisco NAC OS X Agent (read-only client software), which can check antivirus and antispysware definition updates.

After users log in to the Cisco NAC OS X Agent, the agent gets the requirements that are configured for the user role and the operating system from the Cisco ISE server, checks for required packages and sends a report back to the Cisco ISE server. If requirements are met on the client, the user is allowed network access. If requirements are not met, the 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 restricted network access while the user tries to remediate the client system.

### Uninstall the Cisco NAC Agent from Macintosh Clients

You can uninstall the Cisco NAC Agent for Mac OS X clients by running the uninstall script as follows:

- 
- Step 1** Open the navigator pane and navigate to *<local drive ID>* > **Applications**.
  - Step 2** Highlight and right-click the **CCAAgent** icon to bring up the selection menu.
  - Step 3** Choose **Show Package Contents** and double-click **NacUninstall** to uninstall the Cisco NAC Agent on Mac OS X.
- 

## 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.

## Cisco NAC Agent Logs

In the Cisco NAC Agent for Windows, right-click the Agent Tray Icon and then click **Log Packager** to run the support package and collect the agent logs.

In the Cisco NAC Agent for Cisco NAC OS X, in the Tools menu, right-click the Agent icon and click the **Collect Support Logs** option to collect the agent logs and support information. The collected information is available as a zip file. The user can save the file by choosing the file location and filename. By default the file is saved on the desktop with the filename as *CiscoSupportReport.zip*.

If the agent crashes or hangs, you can run the **CCAAgentLogPackager.app** to collect the logs. This file is available at /Applications/CCAAgent.app. You can right-click **CCAAgent.app**, select **Show Package Contents** and double-click **CCAAgentLogPackager** to collect the support information.

## Create an Agent Customization File for the Cisco NAC Agent

An agent customization file allows you to customize the logo, fields, and message text contained in a Cisco NAC Agent screen dialog to suit your specific Windows client network access requirements.

You can create a customization package as a .zip file that contains an XML descriptor file and another .zip file with the contents comprising the customized options.

- 
- Step 1** Assemble the files required to comprise your Agent screen customization package:
- Customized nac\_login.xml file
  - Customized corporate/company logo as a .gif file
  - One or more customized nacStrings\_xx.xml files
  - Customized updateFeed.xml descriptor file
- Step 2** Create a zip file called “brand-win.zip” that contains the assembled files. For example, in a Linux or Unix environment, execute the following: **zip -r brand-win.zip nac\_login.xml nac\_logo.gif nacStrings\_en.xml nacStrings\_cy.xml nacStrings\_el.xml**
- Step 3** Create a “custom.zip” file that contains an appropriate updateFeed.xml descriptor file and the .zip file created above. For example, in a Linux or Unix environment, execute the following: **zip -r custom.zip updateFeed.xml brand-win.zip**
- Step 4** Save the resulting “custom.zip” file to a location on a local machine that you can access when uploading the file to Cisco ISE.
- 

### Custom nac\_login.xml File Template

The nac\_login.xml file is one of the files that is required in your Agent screen customization package, which allows you to customize the logo, fields, and message text contained in a Cisco NAC Agent dialog, like the Properties window, to suit your specific Windows client network access requirements.

Use the following template to construct an appropriate “nac\_login.xml” file to customize the logo, fields, and message text contained in a Cisco NAC Agent screen.

The following example shows a customized file.

```
<tr class="nacLoginMiddleSectionContainerInput">
<td colspan="2">
<fieldset width="100%" id="nacLoginCustomAlert"
style="display:block" class="nacLoginAlertBox">
<table width="100%">
<tr>
<td id="nacLoginCustomAlert.img" valign="top" width="32px">

</td>
<td id="nacLoginCustomAlert.content" class="nacLoginAlertText">
< cues:localize key="login.customalert"/>
</td>
</tr>
</table>
</fieldset>
</td>
</tr>
<tr id="nacLoginRememberMe" style="visibility:hidden">
<td>
< cues:localize key="cd.nbsp"/>
</td>
<td class="cuesLoginField">
<nobr>
<input type="checkbox" alt="" title="" name="rememberme"
id="rememberme" checked="true"/>
< cues:localize key="login.remember_me"/>
</nobr>
</td>
</tr>
```

## Custom nacStrings\_xx.xml File Template

This is one of the files that is required in your Agent screen customization package, allows you to customize the logo, fields, and message text contained in a Cisco NAC Agent dialog, like the Properties screen, to suit your specific Windows client network access requirements.

Use the following template to construct a one or more nacStrings\_xx.xml files, where xx is a two-character identifier for the specific language.

The following example shows a customized nacStrings\_xx.xml file.

```
<cueslookup:appstrings xmlns:cueslookup="http://www.cisco.com/cues/lookup">
<cueslookup:name key="nac.brand.legal_name">Cisco Systems, Inc.</cueslookup:name>
<cueslookup:name key="nac.brand.full_name">Cisco Systems</cueslookup:name>
<cueslookup:name key="nac.brand.short_name">Cisco</cueslookup:name>
<cueslookup:name key="nac.brand.abbreviation">Cisco</cueslookup:name>
<cueslookup:name key="nac.copyright">Copyright </cueslookup:name>
<cueslookup:name key="nac.copyright.period">2009-2013</cueslookup:name>
<cueslookup:name key="nac.copyright.arr">All Rights Reserved</cueslookup:name>
<cueslookup:name key="updateagent.rqst">NAC Agent %1 is available.%br% Do you want to install
this update now?</cueslookup:name>
<cueslookup:name key="updateagent.rqst.retry">Unable to update NAC Agent. Please try
again.</cueslookup:name>
<cueslookup:name key="downloadagent.report">Downloading the update of NAC
Agent.</cueslookup:name>
<cueslookup:name key="downloadagent.packagename.label">Package Name</cueslookup:name>
<cueslookup:name key="downloadagent.completed.label">Completed</cueslookup:name>
<cueslookup:name key="downloadagent.completed.value">%1 of %2 bytes</cueslookup:name>
<cueslookup:name key="downloadagent.speed.label">Speed</cueslookup:name>
<cueslookup:name key="downloadagent.speed.value">%1 bytes/sec</cueslookup:name>
<cueslookup:name key="updateopswat.rqst">NAC Agent Posture component version %1 is
available.%br% Do you want to install this update now?</cueslookup:name>
<cueslookup:name key="updateopswat.rqst.retry">Unable to update NAC Agent Posture component.
Please try again.</cueslookup:name>
<cueslookup:name key="downloadopswat.report">Downloading the update of NAC Agnet Posture
```

```

component.</cueslookup:name>
<cueslookup:name key="login.productname">Education First Compliance Check</cueslookup:name>

<cueslookup:name key="login.version">Version</cueslookup:name>
<cueslookup:name key="login.opswatversion">Posture Component Version</cueslookup:name>
<cueslookup:name key="login.username">Enter your username</cueslookup:name>
<cueslookup:name key="login.password">Enter your PIN</cueslookup:name>
<cueslookup:name key="login.remember_me">Remember Me</cueslookup:name>
<cueslookup:name key="login.server">Server</cueslookup:name>
<cueslookup:name key="login.customalert">Custom EF package version 2.1.1.1 with EF
Logo</cueslookup:name>
<cueslookup:name key="login.Too many users using this account">This account is already
active on another device</cueslookup:name>
<cueslookup:name key="login.differentuser">Login as Different User</cueslookup:name>
<cueslookup:name key="login.removeoldest">Remove Oldest Login Session</cueslookup:name>
<cueslookup:name key="menu_devtools">Dev Tools</cueslookup:name>
<cueslookup:name key="c.sso.ad">Performing Windows Domain automatic login for
NAC</cueslookup:name>
<cueslookup:name key="c.sso.generic">Unknown authentication type</cueslookup:name>
<cueslookup:name key="c.sso.macauth">Performing device filter automatic login for
NAC</cueslookup:name>
<cueslookup:name key="c.sso.vpn">Performing automatic login into NAC environment for remote
user</cueslookup:name>
<cueslookup:name key="c.title.status.authenticating">Authenticating User</cueslookup:name>

<cueslookup:name key="c.title.status.answeringchallenge">Sending Response</cueslookup:name>

<cueslookup:name key="c.title.status.checking">Checking Requirements</cueslookup:name>
<cueslookup:name key="c.title.status.checkcomplete">System Check Complete</cueslookup:name>

<cueslookup:name key="c.title.status.loggedin">NAC Process Completed</cueslookup:name>
<cueslookup:name key="c.title.status.netaccess.none">NAC Process Completed</cueslookup:name>

<cueslookup:name key="c.title.status.netpolicy">Network Usage Policy</cueslookup:name>
<cueslookup:name key="c.title.status.properties">Agent Properties &
Information</cueslookup:name>
<cueslookup:name key="c.title.status.remediating">Remediating System</cueslookup:name>
<cueslookup:name key="c.title.status.session.expired">Session has Expired</cueslookup:name>

<cueslookup:name key="c.title.status.update.available">Update Agent</cueslookup:name>
<cueslookup:name key="c.title.status.update.downloading">Downloading Agent</cueslookup:name>

<cueslookup:name key="c.title.status.update.opswat.available">Update Posture
Component</cueslookup:name>
<cueslookup:name key="c.title.status.update.opswat.downloading">Downloading Posture
Component</cueslookup:name>
<cueslookup:name key="scanning">Checking</cueslookup:name>
<!-- <cueslookup:name key="scanningitemcomplete">Finished Checking</cueslookup:name -->
<cueslookup:name key="ph.about">About</cueslookup:name>
<cueslookup:name key="ph.cancel">Cancel</cueslookup:name>
<!-- <cueslookup:name key="ph.details">Details</cueslookup:name -->
<cueslookup:name key="ph.logout">Logout</cueslookup:name>
<cueslookup:name key="title_remediating">Remediating System</cueslookup:name>
<cueslookup:name key="title_check_complete">System Check Complete</cueslookup:name>
<cueslookup:name key="title_full_access_granted">Logged In</cueslookup:name>
<cueslookup:name key="title_access_denied">Network Access Denied</cueslookup:name>
<cueslookup:name key="tempNetAccess">Temporary Network Access</cueslookup:name>
<cueslookup:name key="announcePleaseBePatient">Please be patient while your system is checked
against the network security policy
</cueslookup:name>
<cueslookup:name key="bbtn.accept">Accept</cueslookup:name>
<cueslookup:name key="bbtn.apply">Apply</cueslookup:name>
<cueslookup:name key="bbtn.cancel">Cancel</cueslookup:name>
<cueslookup:name key="bbtn.continue">Update Later</cueslookup:name>
<cueslookup:name key="bbtn.close">Close</cueslookup:name>
<cueslookup:name key="bbtn.detailshide">Hide Compliance</cueslookup:name>
<cueslookup:name key="bbtn.detailsshow">Show Compliance</cueslookup:name>
<cueslookup:name key="bbtn.download">Download</cueslookup:name>
<cueslookup:name key="bbtn.guestAccess">Guest Access</cueslookup:name>
<cueslookup:name key="bbtn.go2link">Go To Link</cueslookup:name>
<cueslookup:name key="bbtn.launch">Launch</cueslookup:name>
<cueslookup:name key="bbtn.login">Log In</cueslookup:name>
<cueslookup:name key="bbtn.next">Re-Scan</cueslookup:name>

```

```

<cueslookup:name key="bbtn.ok">OK</cueslookup:name>
<cueslookup:name key="bbtn.propertieshide">Hide Properties</cueslookup:name>
<cueslookup:name key="bbtn.reject">Reject</cueslookup:name>
<cueslookup:name key="bbtn.remediate">Repair</cueslookup:name>
<cueslookup:name key="bbtn.rescan">Rescan</cueslookup:name>
<cueslookup:name key="bbtn.reset">Reset</cueslookup:name>
<cueslookup:name key="bbtn.restrictedNet">Get Restricted NET access This one comes down
from the network</cueslookup:name>
<cueslookup:name key="bbtn.savereport">Save Report</cueslookup:name>
<cueslookup:name key="bbtn.skip">Skip</cueslookup:name>
<cueslookup:name key="bbtn.skipao">Skip All Optional</cueslookup:name>
<cueslookup:name key="bbtn.submit">Submit</cueslookup:name>
<cueslookup:name key="bbtn.update">Update</cueslookup:name>
<cueslookup:name key="cd.days">
days
</cueslookup:name>
<cueslookup:name key="cd.nbsp">

</cueslookup:name>
<cueslookup:name key="cd.tempNetAccess.counting">
There is approximately %1 left until your temporary network access expires
</cueslookup:name>
<cueslookup:name key="cd.tempNetAccess.expired">
Your Temporary Network Access has Expired!
</cueslookup:name>
<cueslookup:name key="cd.tempNetAccessShort.counting">
%1 left
</cueslookup:name>
<cueslookup:name key="cd.tempNetAccessShort.expired">
Expired!
</cueslookup:name>
<cueslookup:name key="cd.window.counting">
This window will close in %1 secs
</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess">
Full Network Access
</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess.verbose">
Your device conforms with all the security policies for this protected
network
</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccessWarn.verbose">
Only optional requirements are failing.
It is recommended that you update your system at
your earliest convenience.
</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.progress.verbose">
Refreshing IP address. Please Wait...
</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.complete.verbose">
Refreshing IP address succeeded.
</cueslookup:name>
<cueslookup:name key="dp.status.vlanchange.progress.verbose">
Connecting to protected Network. Please Wait...
</cueslookup:name>
<cueslookup:name key="dp.status.guestNetAccess">
Guest Network Access
</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess">
Network Access Denied
</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess.verbose">
There is at least one mandatory requirement failing.
You are required to update your system before
you can access the network.
</cueslookup:name>
<cueslookup:name key="dp.status.rejectNetPolicy.verbose">
Network Usage Terms and Conditions are rejected. You will not be
allowed to access the network.
</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess">
Restricted Network Access granted.
</cueslookup:name>

```

```

<cueslookup:name key="dp.status.RestrictedNetAccess.verbose">
You have been granted restricted network access because your device
did not conform with all the security policies for this protected
network and you have opted to defer updating your system. It is recommended
that you update your system at your earliest convenience.
</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess">
Temporary Network Access
</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess.bepatient.verbose">
Please be patient while your system is checked against the network security policy.
</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure">
Performing Re-assessment
</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure.verbose">
There is at least one mandatory requirement failing.
You are required to update your system otherwise
your network access will be restricted.
</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure">
Performing Re-assessment
</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure.verbose">
Only optional requirements are failing.
It is recommended that you update your system at
your earliest convenience.
</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout">
Logged out
</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout.verbose">
Temporary Access to the network has expired.
</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated">
Logged out
</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated.verbose">

</cueslookup:name>
<cueslookup:name key="ia.status.checkcomplete">
Finished Checking Requirements
</cueslookup:name>
<cueslookup:name key="ia.status.check.inprogress">
Please be patient while we determine if your system is compliant with the security policy
</cueslookup:name>
<cueslookup:name key="ia.status.check.inprogress.01">
Checking %1 out of %2
</cueslookup:name>
<cueslookup:name key="ia.status.netpolicy">
Access to the network requires that you view and accept the following
Network Usage Policy
</cueslookup:name>
<cueslookup:name key="ia.status.netpolicylinktxt">
Network Usage Policy Terms and Conditions
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.inprogress">
Remediating
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.start">
Please Remediate
</cueslookup:name>
<cueslookup:name key="ia.status.remediate.checkinprogress">
Checking for compliance with Requirement
</cueslookup:name>
<cueslookup:name key="ia.table.name">
Name
</cueslookup:name>
<cueslookup:name key="ia.table.location">
Location
</cueslookup:name>
<cueslookup:name key="ia.table.software">
Software

```



```

</cueslookup:name>
<cueslookup:name key="ia.table.software.programs">
program(s)
</cueslookup:name>
<cueslookup:name key="ia.table.update">
Update
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.nochange">
Do not change current setting
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.notifybeforedownload">
Notify before download
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.notifybeforeinstall">
Notify before install
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.scheduledinstallation">
Download and installation
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcenotifybeforedownload">
Change to notify before download
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcenotifybeforeinstall">
Change to notify before installation
</cueslookup:name>
<cueslookup:name key="ia.table.locationcode.forcescheduledinstall">
Change to download and installation
</cueslookup:name>
<cueslookup:name key="ia.table.description">
Description
</cueslookup:name>
<cueslookup:name key="scs.table.title">
Security Compliance Summary
</cueslookup:name>
<cueslookup:name key="scs.table.header1.scan_rslt">
Scan Result
</cueslookup:name>
<cueslookup:name key="scs.table.header1.pack_name">
Requirement Name
</cueslookup:name>
<cueslookup:name key="scs.table.header1.pack_details">
Requirement Description - Remediation Suggestion
</cueslookup:name>
<cueslookup:name key="scs.table.data.mandatory">
Mandatory
</cueslookup:name>
<cueslookup:name key="scs.table.data.optional">
Optional
</cueslookup:name>
<cueslookup:name key="scs.table.data.pass">
Passed
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_download">
Please download and install the optional software before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_download">
Please download and install the required software before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_launch">
Please launch the optional remediation program(s) before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_launch">
Please launch the required remediation program(s) before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_opswat_av">
Please update the virus definition file of the specified antivirus software before accessing
the network (optional)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_opswat_av">
Please update the virus definition file of the specified antivirus software before accessing
the network (required)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_opswat_as">

```

```

Please update the spyware definition file of the specified anti-spyware software before
accessing the network (optional)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_opswat_as">
Please update the spyware definition file of the specified anti-spyware software before
accessing the network (required)
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_optional_win_update">
Please download and install the optional windows updates before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_mandatory_win_update">
Please download and install the required windows updates before accessing the network
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_launch_prog">
Launching Remediation Program(s)...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_launch_url">
Launching Remediation URL...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_opswat_av">
Updating Virus Definition...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_opswat_as">
Updating Spyware Definition...
</cueslookup:name>
<cueslookup:name key="ia.rem_inst_auto_win_update">
Launching Windows auto Update(s)...
</cueslookup:name>
<cueslookup:name key="ia.rem_launch_downloaded_file">
Downloaded at %1. %br% Please open this folder & double-click executable file to
install the required software.
</cueslookup:name>
<cueslookup:name key="discoveryhost.label">
Discovery Host
</cueslookup:name>
<cueslookup:name key="properties.table.title">
List of Antivirus & Anti-Spyware Products Detected by the Agent
</cueslookup:name>
<cueslookup:name key="properties.table.header1.index">
No.
</cueslookup:name>
<cueslookup:name key="properties.table.header1.description">
Description
</cueslookup:name>
<cueslookup:name key="properties.table.header1.value">
Value
</cueslookup:name>
<cueslookup:name key="properties.table.data.product_type">
Product Type
</cueslookup:name>
<cueslookup:name key="properties.table.data.product_name">
Product Name
</cueslookup:name>
<cueslookup:name key="properties.table.data.product_version">
Product Version
</cueslookup:name>
<cueslookup:name key="properties.table.data.def_version">
Definition Version
</cueslookup:name>
<cueslookup:name key="properties.table.data.def_date">
Definition Date
</cueslookup:name>
<cueslookup:name key="reboot.mandatory.001">
Mandatory System Reboot Required
</cueslookup:name>
<cueslookup:name key="reboot.optional.001">
You need to reboot your system in order for the changes to take effect.
</cueslookup:name>
<cueslookup:name key="rem.error.001">
Unable to remediate particular requirement
</cueslookup:name>
<cueslookup:name key="rem.error.av_access_denied">
The remediation you are attempting is reporting an access denied error. This is usually due

```

```

to a privilege issue. Please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_buffer_too_small">
The remediation you are attempting has failed with an internal error. Please contact your
system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_elevation_required">
The remediation you are attempting requires elevation. Please contact your system
administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_failed">
The remediation you are attempting had a failure. If the problem persists contact your
system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_internal_error">
The remediation you are attempting has reported an internal error. If this problem persists
please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_not_implemented">
The remediation you are attempting is not implemented for this product. Please contact your
system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_not_supported">
The remediation you are attempting is not supported for this product. Please contact your
system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_update_faile">
The AV/AS update has failed. Please try again and if this message continues to display
contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_update_failed_due_to_network">
The AV/AS update failed due to a networking issue. Please try again and if this message
continues to display contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.av_timeout">
The remediation you are attempting has timed out waiting for the operation to finish. If
this continues please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.file_dist_size_error">
The size of the downloaded file does not match the package! Please discard downloaded file
and check with your administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.file_is_not_signed">
The file that has been requested was not digitally signed. Please try again and if this
message continues to display contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.file_save_location_error">
The location for the file to be saved to can not be written. Please choose a different
location.
</cueslookup:name>
<cueslookup:name key="rem.error.http_file_not_found">
The requested file is not found. Please try again and if this problem persists, contact
your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.launch_file_not_found">
The file that has been requested could not be launched either because it could not be found
or there was a problem launching it. Please contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.malformed_URL">
The file that is trying to be downloaded has an incorrect URL. Please contact your system
administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.network_error">
There has been a network error, please try the remediation again. If this message continues
to be seen contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.update_fail_for_non_admin">
The remediation you are trying to do can not be accomplished at your user level. Please
contact your system administrator.
</cueslookup:name>
<cueslookup:name key="rem.error.wsus_search_failure">
The WSUS search failed. This is probably due to a network issue. Please try again and if
this message continues to display contact your system administrator.

```

```

</cueslookup:name>
<cueslookup:name key="server.error.generic">
Agent encountered problems logging user
</cueslookup:name>
<cueslookup:name key="server.error.255">
Network Error: NAC Server could not establish a secure connection to NAC Manager.
This could be due to one or more of the following reasons:
1) NAC Manager certificate has expired or
2) NAC Manager certificate cannot be trusted or
3) NAC Manager cannot be reached or
4) NAC Manager is not responding
Please report this to your network administrator.
</cueslookup:name>
<cueslookup:name key="server.error.5000">
Invalid provider name
</cueslookup:name>
<cueslookup:name key="server.error.5001">
Failed to add user to online list
</cueslookup:name>
<cueslookup:name key="server.error.5002">
Server communication error
</cueslookup:name>
<cueslookup:name key="server.error.5003">
Invalid username or password
</cueslookup:name>
<cueslookup:name key="server.error.5004">
Unknown user
</cueslookup:name>
<cueslookup:name key="server.error.5005">
Account expired
</cueslookup:name>
<cueslookup:name key="server.error.5006">
Account currently disabled
</cueslookup:name>
<cueslookup:name key="server.error.5007">
Exceed quota limit
</cueslookup:name>
<cueslookup:name key="server.error.5008">
Insufficient Clean Access packages installed
</cueslookup:name>
<cueslookup:name key="server.error.5009">
Access to network is blocked by the administrator
</cueslookup:name>
<cueslookup:name key="server.error.5010">
Vulnerabilities not fixed
</cueslookup:name>
<cueslookup:name key="server.error.5011">
This client version is old and not compatible. Please login from web browser to see the
download link for the new version.
</cueslookup:name>
<cueslookup:name key="server.error.5012">
Network policy is not accepted
</cueslookup:name>
<cueslookup:name key="server.error.5013">
Invalid switch configuration
</cueslookup:name>
<cueslookup:name key="server.error.5014">
Too many users using this account
</cueslookup:name>
<cueslookup:name key="server.error.5015">
Invalid session
</cueslookup:name>
<cueslookup:name key="server.error.5016">
Null session
</cueslookup:name>
<cueslookup:name key="server.error.5017">
Invalid user role
</cueslookup:name>
<cueslookup:name key="server.error.5018">
Invalid login page
</cueslookup:name>
<cueslookup:name key="server.error.5019">
Encoding failure

```

```

</cueslookup:name>
<cueslookup:name key="server.error.5020">
A security enhancement is required for your Agent. Please upgrade your Agent or contact
your network administrator.
</cueslookup:name>
<cueslookup:name key="server.error.5021">
Can not find server reference
</cueslookup:name>
<cueslookup:name key="server.error.5022">
User role currently disabled
</cueslookup:name>
<cueslookup:name key="server.error.5023">
Authentication server is not reachable
</cueslookup:name>
<cueslookup:name key="server.error.5024">
Agent user operating system is not supported
</cueslookup:name>
<cueslookup:name key="server.error.generic_emergency">
The Agent has encountered an unexpected error and is restarting.
</cueslookup:name>
<cueslookup:name key="server.error.http_error">
Clean Access Server is not available on the network.
</cueslookup:name>
<cueslookup:name key="server.error.nw_interface_chg">
Authentication interrupted due to network status change. Press OK to retry.
</cueslookup:name>
<cueslookup:name key="server.error.svr_misconfigured">
Clean Access Server is not properly configured.
</cueslookup:name>
<cueslookup:name key="server.clarification.generic_emergency">
Please contact your administrator if the problem persists.
</cueslookup:name>
<cueslookup:name key="announce.savingreport">
Saving Report
</cueslookup:name>
<cueslookup:name key="announce.savingreport.failed">
Unable to save report
</cueslookup:name>
<cueslookup:name key="announce.cancelremediationack">
Clicking Cancel may change your network connectivity and interrupt download or required
updates.<p> Do you want to continue?</p>
</cueslookup:name>
<cueslookup:name key="announce.dismiss.default">
Dismiss to continue
</cueslookup:name>
<cueslookup:name key="announce.logoutconfirm">
Successsfully logged out from the network!
</cueslookup:name>
</cueslookup:appstrings>

```

**Note**

There is no limit to the number of characters you can use for the customized text. However, Cisco recommends restricting the length so that these fields do not take up too much space in the resulting customized login screen as it appears on the client.

## Sample Extended nacStrings\_xx.xml File

```

<cueslookup:name key="dp.status.fullNetAccess">Full Network Access</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccess.verbose">Your device conforms with all the
security policies for this protected network</cueslookup:name>
<cueslookup:name key="dp.status.fullNetAccessWarn.verbose">Only optional requirements are
failing. It is recommended that you update your system at your earliest
convenience.</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.progress.verbose">Refreshing IP address. Please
Wait ...</cueslookup:name>
<cueslookup:name key="dp.status.iprefresh.complete.verbose">Refreshing IP address

```

```

succeeded.</cueslookup:name>
<cueslookup:name key="dp.status.vlanchange.progress.verbose">Connecting to protected Network.
Please Wait ...</cueslookup:name>
<cueslookup:name key="dp.status.guestNetAccess">Guest Network Access</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess">Network Access Denied</cueslookup:name>
<cueslookup:name key="dp.status.noNetAccess.verbose">There is at least one mandatory
requirement failing. You are required to update your system before you can access the
network.
</cueslookup:name><cueslookup:name key="dp.status.rejectNetPolicy.verbose">Network Usage
Terms and Conditions are rejected. You will not be allowed to access the
network.</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess">Restricted Network Access
granted.</cueslookup:name>
<cueslookup:name key="dp.status.RestrictedNetAccess.verbose">You have been granted restricted
network access because your device did not conform with all the security policies for this
protected network and you have opted to defer updating your system. It is recommended that
you update your system at your earliest convenience.</cueslookup:name>
<cueslookup:name key="dp.status.temporaryNetAccess">Temporary Network Access</cueslookup:name>

<cueslookup:name key="dp.status.temporaryNetAccess.bepatient.verbose">Please be patient
while your system is checked against the network security policy.</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure">Performing
Re-assessment</cueslookup:name>
<cueslookup:name key="dp.status.pra.mandatoryfailure.verbose">There is at least one mandatory
requirement failing. You are required to update your system otherwise your network access
will be restricted.</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure">Performing
Re-assessment</cueslookup:name>
<cueslookup:name key="dp.status.pra.optionalfailure.verbose">Only optional requirements are
failing. It is recommended that you update your system at your earliest
convenience.</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout">Logged out</cueslookup:name>
<cueslookup:name key="dp.status.SessionTimeout.verbose">Temporary Access to the network has
expired.</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated">Logged out</cueslookup:name>
<cueslookup:name key="dp.status.Unauthenticated.verbose"> </cueslookup:name>

```

## UpdateFeed.xml Descriptor File Template

This is one of the files that is required in your Agent screen customization package, allows you to customize the logo, fields, and message text contained in a Cisco NAC Agent dialog, like the Properties screen, to suit your specific Windows client network access requirements.

Before you can complete your Agent screen customization package, you must construct a suitable updateFeed.xml XML descriptor file. Use the following example as a template to set up the updateFeed.xml descriptor file required for your customization package.

```

<?xml version="1.0" encoding="utf-8"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:update="http://www.cisco.com/cpm/update/1.0">

<title>Provisioning Update</title>
<updated>2011-12-21T12:00:00Z</updated>
<id>https://www.cisco.com/web/secure/pmbu/provisioning-update.xml</id>
<author>
<name>Cisco Support</name>
<email>support@cisco.com</email>
</author>
<!-- Custom Branding -->
<entry>
<id>http://foo.foo.com/foo/AgentCustomizationPackage/1/1/1/7</id>
<title>Agent Customization Package</title>
<updated>2010-06-07T12:00:00Z</updated>
<summary>This is EF Agent Customization Package 1.1.1.7</summary>
<link rel="enclosure" type="application/zip" href="brand-win.zip" length="18884" />
<update:type>AgentCustomizationPackage</update:type>
<update:version>1.1.1.7</update:version>
<update:os>WINDOWS_ALL</update:os>
</entry>
</feed>

```

Note the following points while creating the updateFeed.xml descriptor file:

- `<update:os>`—You must always set this attribute to “WINDOWS\_ALL” to include all the Windows OS versions that are supported by Cisco NAC Agent. See [Support Information for Cisco NAC Appliance Agents](#) for the list of Windows OS versions that are supported by Cisco NAC Agent.
- `<update:version>`—This refers to the Agent Customization Package version that you want to upgrade to. This value should be four digit `<n.n.n.n>` and should be greater than the package version that is currently installed.
- `<id>`—This id can be anything, but should be unique for each Agent Customization Package.

## Example XML File Generated Using the Create Profile Function

```
<?xml version="1.0" ?>
<cfg>
 <VlanDetectInterval>0</VlanDetectInterval>
 <RetryDetection>3</RetryDetection>
 <PingArp>0</PingArp>
 <PingMaxTimeout>1</PingMaxTimeout>
 <EnableVlanDetectWithoutUI>0</EnableVlanDetectWithoutUI>
 <SignatureCheck>0</SignatureCheck>
 <DisableExit>0</DisableExit>
 <PostureReportFilter>displayFailed</PostureReportFilter>
 <BypassSummaryScreen>1</BypassSummaryScreen>
 <LogFileSize>5</LogFileSize>
 <DiscoveryHost></DiscoveryHost>
 <DiscoveryHostEditable>1</DiscoveryHostEditable>
 <Locale>default</Locale>
 <AccessibilityMode>0</AccessibilityMode>
 <SwissTimeout>1</SwissTimeout>
 <HttpDiscoveryTimeout>30</HttpDiscoveryTimeout>
 <HttpTimeout>120</HttpTimeout>
 <ExceptionMACList></ExceptionMACList>
 <GeneratedMAC></GeneratedMAC>
 <AllowCRLChecks>1</AllowCRLChecks>
 <DisableL3SwissDelay>0</DisableL3SwissDelay>
 <ServerNameRules></ServerNameRules>
</cfg>
```



### Note

This file also contains two static (that is, uneditable by the user or Cisco ISE administrator) “AgentCfgVersion” and “AgentBrandVersion” parameters used to identify the current version of the agent profile and agent customization file, respectively, on the client.

## 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 it 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.

For Cisco ISE NAC agents, resources can be selected from the client provisioning policy page.

### 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.

- 
- 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 iOS", 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)."
- 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.



## 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, page 565](#)
- [Posture Administration Settings, page 568](#)
- [Download Posture Updates to Cisco ISE, page 572](#)
- [Configure Acceptable Use Policies for Posture Assessment, page 573](#)
- [Configure Posture Policies, page 573](#)
- [Posture Assessment Options, page 574](#)
- [Posture Remediation Options, page 575](#)
- [Custom Conditions for Posture, page 576](#)
- [Custom Posture Remediation Actions, page 576](#)
- [Posture Assessment Requirements, page 581](#)
- [Custom Permissions for Posture, page 584](#)
- [Configure Standard Authorization Policies, page 584](#)

### Posture Service

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.

Clients interact with the posture service through the AnyConnect ISE Posture Agent or Network Admission Control (NAC) Agent on the endpoint to enforce security policies, meet compliance, and allow the endpoint to gain access to your protected network. Client Provisioning ensures 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. This is because there is no clear disconnect of the older user. When a new user is sent, the Agent

is hung on the old user process and session ID, and hence a new posture session cannot take place. As per the Microsoft Security policies, it is recommended to disable Fast User Switching.

## 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:

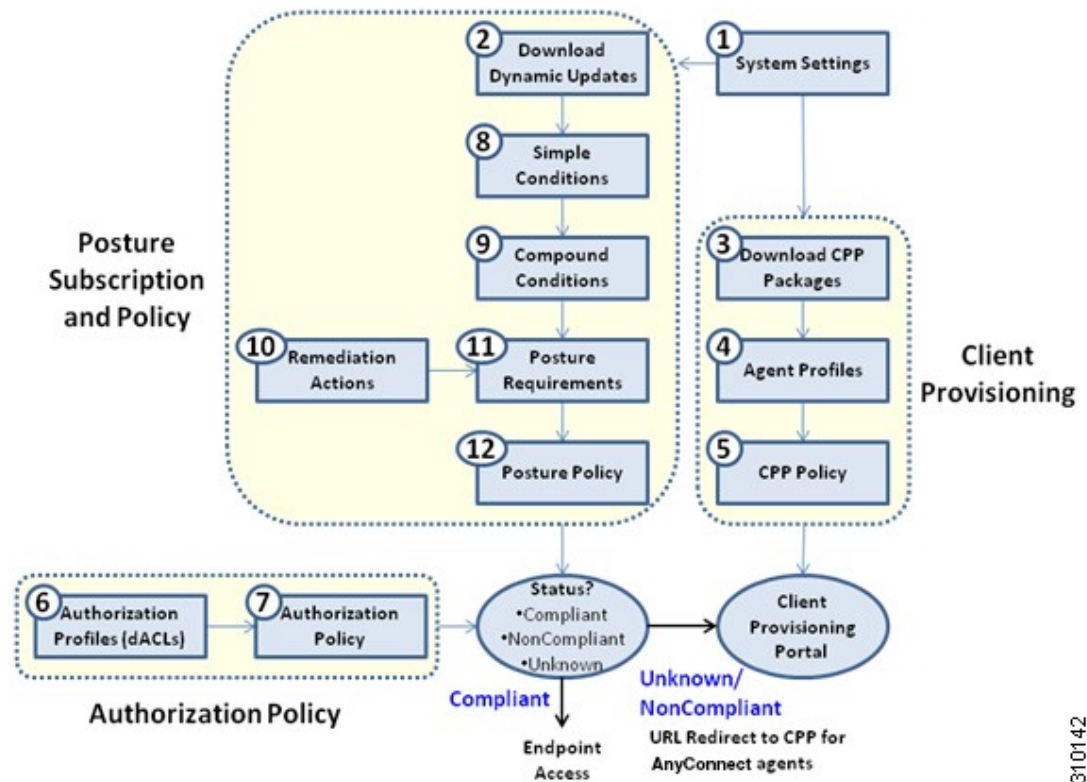
- 1 via HTTP to Port 80 on a Cisco ISE server (if configured)
- 2 via HTTPS to Port 8905 on a Cisco ISE server (if configured)
- 3 via HTTP to Port 80 on the default gateway
- 4 via HTTPS to Port 8905 to each previously contact server
- 5 via HTTP to Port 80 on enroll.cisco.com

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

Figure 44: Posture and Client Provisioning Policies Workflow in Cisco ISE



310142

## Posture Service Licenses

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 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, or as an inline posture node as needed. 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) or an Inline Posture node.
- 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 page.
- Step 3** Click **Edit**.
- 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 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** Click the **Time Range** drop-down arrow and select the specific time period.
- Step 3** Click **Run** to view the summary of all the endpoints that logged on for a selected period of time.
- 

## 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.

## 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 **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 **Administration > System > Settings > Posture > General Settings** configuration page.

### 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** Enter a time value in minutes, in the **Remediation Timer** field.  
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 Screen 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 screen 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 Non-Agent 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**, 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.

### 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 the following:
  - Update the existing PRA configuration with the *Any* user identity group to reflect a user identity group other than *Any*.
  - or
  - Delete the existing PRA configuration with a user identity group “*Any*”.

- 
- Step 1** Choose **Administration > System > Settings > Posture > Reassessments**.
  - Step 2** Click **Add**.
  - Step 3** Modify the values in the **New Reassessment Configuration** page to create a new PRA.
  - Step 4** Click **Submit** to create a PRA configuration.
-

## 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 on 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.  
Once 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.
- 

## 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**.
- 

**Configure Posture Policies**

A posture policy is a collection of posture requirements, which are associated with one or more identity groups, and operating systems. The Dictionary Attributes are optional conditions in conjunction with the identity groups and the operating systems that allow you to define different policies for the clients.

**Before You Begin**

- You must have an understanding of acceptable use policy (AUP).

- You must have an understanding of periodic reassessments (PRA).

- 
- Step 1** Choose **Policy > Posture**.
- Step 2** Choose the **Status** type.
- Step 3** In the **Rule Name** text box, enter the policy name.  
It is a best practice to configure posture policy with each requirement as a separate rule, to avoid unexpected results.
- Step 4** From **identity Groups**, choose the role.
- Step 5** From **Operating Systems**, choose the operating system.
- Step 6** 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 visible while configuring an authorization policy.
- Step 7** From **Requirements**, choose a requirement. You can also create a new Requirement.
- Step 8** Click **Done**.
- Step 9** Click **Save**.
- 

## 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 38: Posture Assessment Options**

ISE Posture Agent for Windows	Web Agent for Windows	ISE Posture Agent for Macintosh OS X
Operating System/Service Packs/Hotfixes	Operating System/Service Packs/Hotfixes	—
Service Check	Service Check	Service Check (AC 4.1 and ISE 1.4)
Registry Check	Registry Check	—
File Check	File Check	File Check (AC 4.1 and ISE 1.4)
Application Check	Application Check	Application Check (AC 4.1 and ISE 1.4)
Antivirus Installation	Antivirus Installation	Antivirus Installation
Antivirus Version/ Antivirus Definition Date	Antivirus Version/ Antivirus Definition Date	Antivirus Version/ Antivirus Definition Date

ISE Posture Agent for Windows	Web Agent for Windows	ISE Posture Agent for Macintosh OS X
Antispyware Installation	Antispyware Installation	Antispyware Installation
Antispyware Version/ Antispyware Definition Date	Antispyware Version/ Antispyware Definition Date	Antispyware Version/ Antispyware Definition Date
Patch Management Check (AC 4.1 and ISE 1.4)	—	Patch Management Check (AC 4.1 and ISE 1.4)
Windows Update Running	Windows Update Running	—
Windows Update Configuration	Windows Update Configuration	—
WSUS Compliance Settings	WSUS Compliance Settings	—

## 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 39: Posture Remediation Options**

ISE Posture Agent for Windows	Web Agent for Windows	ISE Posture Agent for Macintosh OS X
Message Text (Local Check)	Message Text (Local Check)	Message Text (Local Check)
URL Link (Link Distribution)	URL Link (Link Distribution)	URL Link (Link Distribution)
File Distribution	File Distribution	—
Launch Program	—	—
Antivirus Definition Update	—	Antivirus Live Update
Antispyware Definition Update	—	Antispyware Live Update
Windows Update	—	—
WSUS	—	—

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 40: Posture Remediation Options**

<b>ISE Posture Agent for Windows</b>	<b>Web Agent for Windows</b>	<b>ISE Posture Agent for Macintosh OS X</b>
Message Text (Local Check)	Message Text (Local Check)	Message Text (Local Check)
URL Link (Link Distribution)	URL Link (Link Distribution)	URL Link (Link Distribution)
File Distribution	File Distribution	—
Launch Program	—	—
Antivirus Definition Update	—	Antivirus Live Update
Antispyware Definition Update	—	Antispyware Live Update
Patch Management Remediation (AC 4.1 - and ISE 1.4)	—	—
Windows Update	—	—
WSUS	—	—

## 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".

## 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.

## 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** Modify the values in the **New File Remediation** page.
  - Step 6** 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**.
  - Step 3** Click **Patch Mangement Remediation**.
  - Step 4** Click **Add**.
  - Step 5** Modify the values in the **Patch Management Remediation** page.
  - Step 6** Click **Submit** to add the remediation action to the **Patch Management Remediations** page.
- 

## 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.

- 
- Step 1** Choose **Policy > Policy Elements > Results > Posture**.
  - Step 2** Click **Remediation Actions**.
  - Step 3** Click **AV Remediation**.
  - Step 4** Click **Add**.
  - Step 5** Modify the values in the **New AV Remediation** page.
  - Step 6** Click **Submit**.
- 

## 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.

- 
- Step 1** Choose **Policy > Policy Elements > Results > Posture**.
  - Step 2** Click **Remediation Actions**.
  - Step 3** Click **AS Remediation**.
  - Step 4** Click **Add**.
  - Step 5** Modify the values in the **New AS Remediations** page.
  - Step 6** Click **Submit**.
- 

## 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.`

## Windows Update Remediation

Windows update remediation ensures that Automatic Updates configuration is turned on Windows clients per your security policy. Windows administrators have an option to turn on or turn off Automatic Updates on Windows clients. Microsoft Windows uses this feature to check for updates regularly. If the Automatic Updates feature is turned on, then Windows automatically updates Windows-recommended updates before any other updates.

The Windows Automatic Updates setting will differ for different Windows operating systems.

For example, Windows XP provides the following settings for configuring Automatic Updates:

- Automatic (recommended)—Windows allows clients to download recommended Windows updates and install them automatically
- Download updates for me, but let me choose when to install them—Windows downloads updates for clients and allows clients to choose when to install updates
- Notify me but don't automatically download or install them—Windows only notifies clients, but does not automatically download, or install updates
- Turn off Automatic Updates—Windows allows clients to turn off the Windows Automatic Updates feature. Here, clients are vulnerable unless clients install updates regularly, which can be done from the Windows Update Web site link.

You can check whether or not the Windows updates service (wuaserv) is started or stopped in any Windows client by using the **pr\_AutoUpdateCheck\_Rule**. This is a predefined Cisco rule, which can be used to create a posture requirement. If the posture requirement fails, the Windows update remediation that you associate to the requirement enforces the Windows client to remediate by using one of the options in Automatic Updates.

## 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.
  - Step 6** Click **Submit**.
-

## 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.

- 
- Step 1** Choose **Policy > Policy Elements > Results > Posture**.
  - Step 2** Click **Remediation Actions**.
  - Step 3** Click **Windows Server Update Services Remediation**.
  - Step 4** Click **Add**.
  - Step 5** Modify the values in the **New Windows Server Update Services Remediation** page.
  - Step 6** Click **Submit**.
- 

## 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.

**Figure 45: Posture Policy Requirement Types**

Status	Rule Name	Identity Groups	Op
✓	Altiris Registry	If Any	and W
✓	Connected Backup Application	If Any	and W
✓	HotFixes_Dummy_Win	If Any	and W
✓	HotFixes_Win7_64bit	If Any	and W
✓	HotFixes_Win_XP	If Any	and W
✓	McAfeeAV_Definition_Win	If Any	and W

### 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.

## 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. This method is not supported in Inline Posture deployments.
  - 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**.

---

## 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 in the Authorization Policy page, standard exceptions 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 > Authorization**.

**Step 2** Choose one of the matching rule type to apply from the drop-down list shown at the top of the Authorization Policy page.

- **First Matched Rule Applies** — This option sets access privileges with a single authorization policy that is first matched during evaluation from the list of standard authorization policies. Once the first matching authorization policy is found, the rest of the standard authorization policies are not evaluated.

- **Multiple Matched Rule Applies**— This option sets access privileges with multiple authorization policies that are matched during evaluation from the list of all the standard authorization policies

**Step 3** Click the down arrow next to **Edit** in the default standard authorization policy row.

**Step 4** Click **Insert New Rule Above**.

**Step 5** Enter a rule name, choose identity groups and other conditions, and associate an authorization profile in the new authorization policy row that appears above the default standard authorization policy row.

**Step 6** Click **Done** to create a new standard authorization policy in read-only mode.

**Step 7** Click **Save**.

---







## Cisco TrustSec Policies Configuration

---

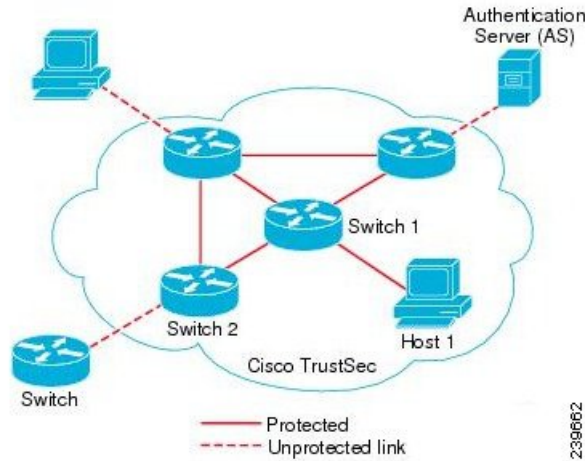
- [TrustSec Architecture, page 587](#)
- [Configure TrustSec Global Settings, page 590](#)
- [Configure TrustSec Devices, page 591](#)
- [Configure TrustSec AAA Servers, page 593](#)
- [Security Groups Configuration, page 594](#)
- [Egress Policy, page 597](#)
- [SGT Assignment, page 602](#)
- [TrustSec Configuration and Policy Push, page 606](#)
- [Run Top N RBACL Drops by User Report, page 615](#)

### 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.

**Figure 46: TrustSec Architecture**



## 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
- **SGT Reservation**—An enhancement in Cisco ISE to reserve a range of SGTs to enable IP to SGT mapping.
- **IP-to-SGT Mapping**—An enhancement in Cisco ISE to bind an endpoint IP to an SGT and provision it to a TrustSec-capable device. Cisco ISE supports entering 1000 IP-to-SGT Mappings.
- **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 41: TrustSec Terminology**

Term	Meaning
Supplicant	A device that tries to join a trusted network.
Authentication	The process of verifying the identity of each device before allowing it to be part of the trusted network.
Authorization	The process of deciding the level of access to a device that requests access to a resource on a trusted network based on the authenticated identity of the device.
Access control	The process of applying access control on a per-packet basis based on the SGT that is assigned to each packet.
Secure communication	The process of encryption, integrity, and data-path replay protection for securing the packets that flow over each link in a trusted network.

Term	Meaning
TrustSec device	Any of the Cisco Catalyst 6000 Series or Cisco Nexus 7000 Series switches that support the TrustSec solution.
TrustSec-capable device	A TrustSec-capable device will have TrustSec-capable hardware and software. For example, the Nexus 7000 Series Switches with the Nexus operating system.
TrustSec seed device	The TrustSec device that authenticates directly against the Cisco ISE server. It acts as both the authenticator and supplicant.
Ingress	When packets first encounter a TrustSec-capable device that is part of a network where the Cisco TrustSec solution is enabled, they are tagged with an SGT. This point of entry into the trusted network is called the ingress.
Egress	When packets pass the last TrustSec-capable device that is part of a network where the Cisco TrustSec solution is enabled, they are untagged. This point of exit from the trusted network is called the egress.

## 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](#).

## 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 **Administration** > **System** > **Settings** > **TrustSec Settings**.
- Step 2** Enter the values in the fields.
- Step 3** Click **Save**.
- 

### What to Do Next

- [Configure TrustSec Devices](#), on page 591

## Configure TrustSec Devices

For Cisco ISE to process requests from TrustSec-enabled devices, you must define these TrustSec-enabled devices in Cisco ISE.

- 
- Step 1** Choose **Administration** > **Network Resources** > **Network Devices**.
- Step 2** Click **Add**.
- Step 3** Enter the required information in the **Network Devices** section.
- Step 4** Check the **Advanced Trustsec Settings** check box to configure a Trustsec-enabled device.
- Step 5** Click **Submit**.
- 

### 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:

## 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 **Administration** > **Network Resources** > **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 **Administration** > **Network Resources** > **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.

## 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 **Administration** > **Network Resources** > **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:

- **Policy > Policy Elements > Results > Trustsec > 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.

### 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 **Policy > Policy Elements > Results > TrustSec > 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** 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 Trustsec global settings page under **Administration > System > Settings > TrustSec Settings**.
  - Step 5** 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 **Policy > Policy Elements > Results > TrustSec > 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 **Policy > Policy Elements > Results > TrustSec > 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 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 **Policy > Policy Elements > Results > TrustSec > 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 all
```

The ACL command should match the syntax of your network device.
- Step 4** Click **Submit**.
-

## 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 **Policy > TrustSec > Egress Policy** page.

You can view the Egress policy in three different ways:

- Source Tree View
- Destination Tree View
- Matrix View

### 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 SGTs 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.

The Matrix view has the same GUI elements as the Source and Destination views. However, it has these additional elements:

## Matrix Dimensions

The **Dimension** drop-down list in the Matrix view enables you to set the dimensions of the matrix.

## Condensed View

The Condensed option in the egress policy matrix view allows you to display the matrix without empty cells. Check the **Condensed** check box to hide empty cells.

## Import/Export Matrix

The **Import** and **Export** buttons enable you to import or export the matrix.

## 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.

- 
- Step 1** Choose **Policy > TrustSec > 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**.
- 

## 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.

### Add the Mapping of Egress Policy Cells

You can add the mapping cell for Egress Policy from the Policy page.

- 
- Step 1** Choose **Policy > TrustSec > 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.
- Step 4** Select appropriate values for:
- Source Security Group
  - Destination Security Group
  - Status, Security Group ACLs
  - Final Catch All Rule
- Step 5** Click **Save**.
-

## Export Egress Policy

- 
- Step 1** Choose **Policy > TrustSec > Egress Policy > Matrix**.
- Step 2** Click **Export**.
- Step 3** Save the CSV file to your local system.
- 

## 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 **Policy > TrustSec > Egress Policy > Matrix**.
- 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 **Stop Import on First Error** check box for Cisco ISE to abort the import if it encounters any errors.
- Step 5** Click **Import**.
-

## Configure SGT from Egress Policy

You can create Security Groups directly from the Egress Policy page.

- 
- Step 1** Choose **Policy > TrustSec > 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

## 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 a 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.

## 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.

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.



## 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 **Policy > TrustSec > 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 **Policy > Authorization**.
- 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.

---

## Add Single IP-to-SGT Mappings

### Before You Begin

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

---

- Step 1** Choose **Policy > Policy Elements > Results > TrustSec > Security Group Mappings > Hosts**.
- Step 2** Click **Add** to add a new single IP-SGT mapping.
- Step 3** Choose if you want to enter the **Hostname** or the **IP Address** of the device. You can also enter the subnet mask for the IP address.
- Step 4** Choose one of the following:
- **Group Mapping**—To set the IP mapping to be part of existing Mapping Group.
  - **Security Group Tag**—To create a flat mapping between this IP and SGT.
- Step 5** Choose the destination network device on which you want to deploy this mapping. You can deploy the mappings on all trustsec devices, on selected network device groups, or on selected network devices.
- Step 6** Click **Submit**.
- 

## Add Group IP-to-SGT Mappings

### Before You Begin

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

---

- Step 1** Choose **Policy > Policy Elements > Results > TrustSec > Security Group Mappings > Groups**.
- Step 2** Click **Add** to add a new group IP-SGT mapping.
- Step 3** Enter a **Name** and a **Description** for the new group.
- Step 4** Enter the **Security Group Tag** to which this group will be mapped to.
- Step 5** Choose the destination network device on which you want to deploy this mapping. You can deploy the mappings on all trustsec devices, on selected network device groups, or on selected network devices.
- Step 6** Click **Submit**.
-

## Import Security Group Mappings Hosts

You can import a list of security group mappings hosts into a Cisco ISE node using a comma-separated value (CSV) file. You cannot run an import of the same resource type at the same time. For example, you cannot concurrently import security group mappings hosts from two different import files.

You can download the CSV template from the **Policy > Policy Elements > Results > Trustsec > Security Group Mappings > Hosts > Import** page. Enter your security group mappings hosts details in the template, and save it as a CSV file, which you can then import this back in to Cisco ISE.

While importing hosts, you can create new records or update existing records. Cisco ISE displays the summary of the number of hosts that are imported and also reports any errors that were found during the import process. When you import hosts, you can also define whether you want Cisco ISE to stop the import process when Cisco ISE encounters the first error.

- 
- Step 1** Choose **Policy > Policy Elements > Results > TrustSec > Security Group Mappings > Hosts**.
  - 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, if required.
  - Step 5** Click **Import**.
- 

## Export Security Group Mappings Hosts

You can export security group mappings hosts configured in Cisco ISE in the form of a CSV file that you can use to import these hosts into another Cisco ISE node.

- 
- Step 1** Choose **Policy > Policy Elements > Results > TrustSec > Security Group Mappings > Hosts**.
  - Step 2** Click **Export**.
  - Step 3** To export security group mappings hosts, you can do one of the following:
    - Check the check boxes next to the hosts that you want to export, and choose **Export > Export Selected**.
    - Choose **Export > Export All** to export all the security group mappings hosts that are defined.
  - Step 4** Save the export.csv file to your local hard disk.
- 

## Deploy IP-to-SGT Mappings

After you add IP-to-SGT mappings to Cisco ISE you must deploy these to the target network device. You must do this explicitly even though you have saved the mappings earlier. Cisco ISE provides you the option to deploy all or only a subset of the mappings.

### Before You Begin

You must have added IP-to-SGT mappings to Cisco ISE or created IP-to-SGT mappings groups that contain IP-to-SGT mappings .

- 
- Step 1** To deploy IP-to-SGT mappings to devices, you can do one of the following:
- Choose **Policy > Policy Elements > Results > Trustsec > Security Group Mappings > Groups**, if you want to deploy IP-to-SGT mapping groups to devices.
  - Choose **Policy > Policy Elements > Results > Trustsec > Security Group Mappings > Hosts**, if you want to deploy single IP-to-SGT mappings to devices.
- Step 2** Do one of the following:
- Check the check box next to the group or mapping that you want to deploy, and choose **Deploy** to deploy only the selected mappings.
  - Choose **Deploy** to deploy all the IP-to-SGT mappings configured in Cisco ISE.

Cisco ISE deploys the mappings to the specific network devices defined in the group or mapping. It also displays a report with details such as deployed devices, configuration, deployment status and failure reason if any.

---

## 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.

### 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 its 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 out on network platforms that support CoA pushing.

- 
- Step 1** Choose **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:

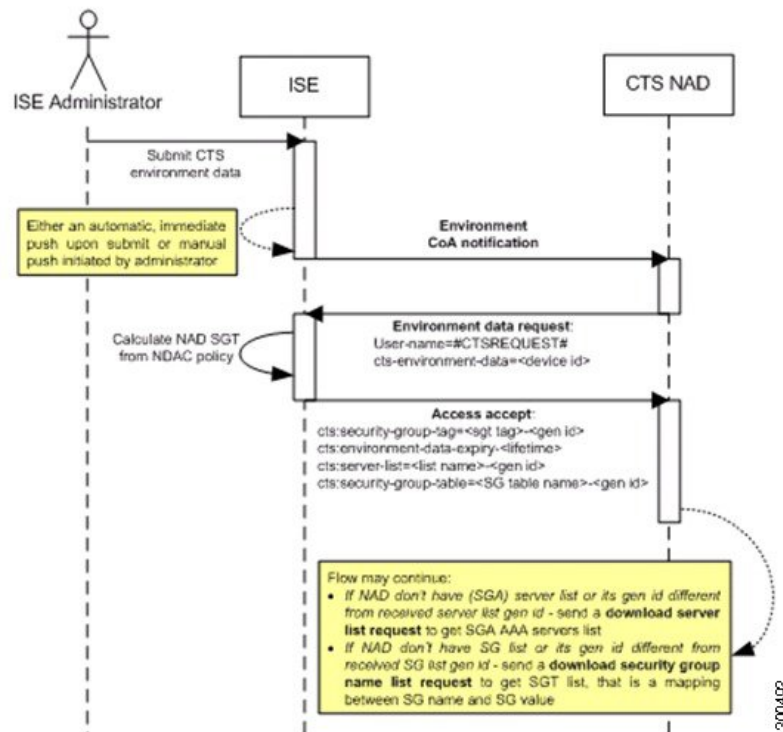
- a) Choose **Device Administration > Network Resources > Network Devices**, and verify the required network device's name, IP address, RADIUS and TrustSec settings are properly configured.
  - b) Scroll down to **Advanced TrustSec Settings**, and in the **TrustSec Notifications and Updates** section, 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 47: 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

#### *Trigger Environment CoA for Network Devices*

To trigger an Environment CoA for the Network devices, complete the following steps:

- 
- Step 1** Choose **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 **Policy > Policy Elements > Results > TrustSec > 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 **Administration > Network Resources > 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

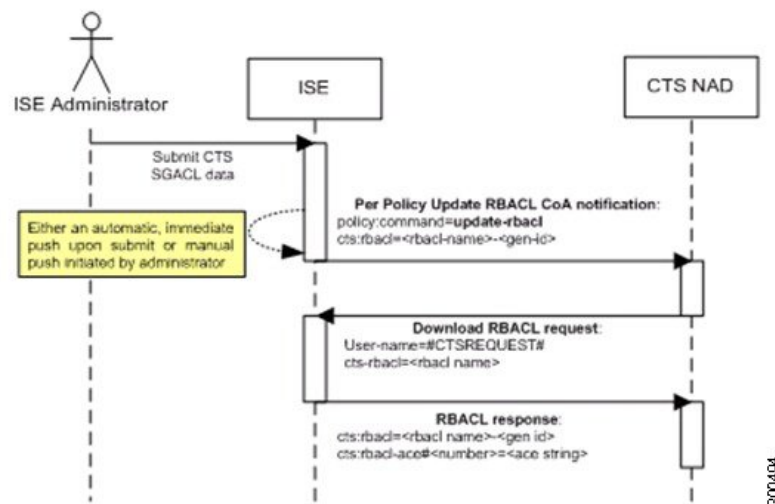
To trigger an Environment CoA for the NDAC Policies, complete the following steps.

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.

**Figure 48: 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

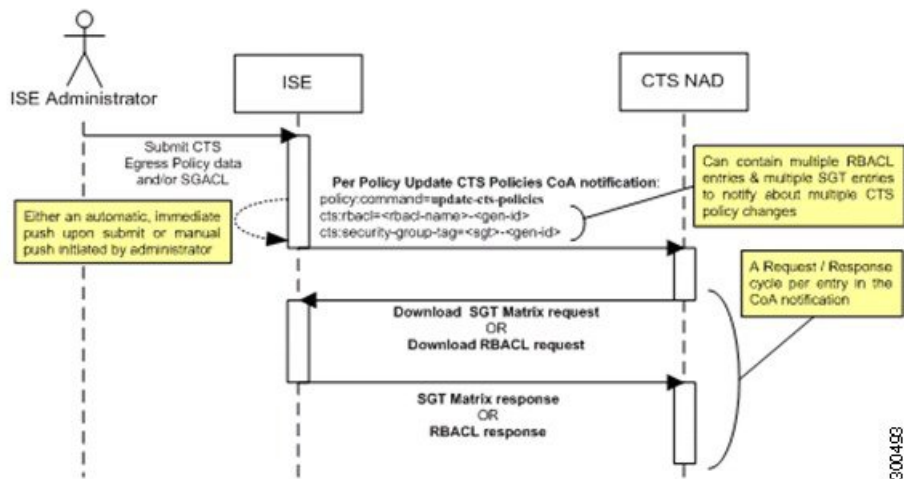
To trigger an Update SGACL Named List CoA, complete the following steps:

- 
- Step 1** Choose **Policy > Policy Elements > Results**.
- Step 2** From the Results navigation pane on the left, click the button next to **TrustSec** and click **Security Group ACLs**.
- Step 3** Change the content of the SGACL. After you submit a SGACL, it promotes the generation ID of the SGACL.
- Step 4** 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.

**Figure 49: 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 reply 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.



## 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 42: TrustSec CoA Summary**

UI Page	Operation that triggers CoA	How it is triggered	CoA type	Send to
Network Device	Changing the environment TTL in the TrustSec section of the page	Upon successful Submit of TrustSec network device	Environment	The specific network device
TrustSec AAA Server	Any change in the TrustSec AAA server (create, update, delete, reorder)	Accumulative changes can be pushed by clicking the Push button on the TrustSec AAA servers list page.	Environment	All TrustSec network devices
Security Group	Any change in the SGT (create, rename, delete)	Accumulative changes can be pushed by clicking the Push button on the SGT list page.	Environment	All TrustSec network devices
NDAC Policy	Any change in the NDAC policy (create, update, delete)	Accumulative changes can be pushed by clicking the Push button on the NDAC policy page.	Environment	All TrustSec network devices
SGACL	Changing SGACL ACE	Accumulative changes can be pushed by clicking the Push button on the SGACL list page.	Update RBACL named list	All TrustSec network devices
	Changing SGACL name or IP version	Accumulative changes can be pushed by clicking the Push button on the SGACL list page or the policy push button in the Egress table.	Update SGT matrix	All TrustSec network devices
Egress Policy	Any operation that changes the generation ID of an SGT	Accumulative changes can be pushed by clicking the Push button on the egress policy page.	Update SGT matrix	All TrustSec network devices

## 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** From the Cisco ISE Admin dashboard, select **Operations > Reports > ISE 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, page 619](#)
- [Reports, page 657](#)







## Monitoring and Troubleshooting

---

- [Monitoring and Troubleshooting Service in Cisco ISE, page 619](#)
- [Device Configuration for Monitoring, page 621](#)
- [Network Process Status, page 621](#)
- [Network Authentications, page 622](#)
- [Profiler Activity and Profiled Endpoints, page 622](#)
- [Troubleshooting the Profiler Feed, page 623](#)
- [Posture Compliance, page 623](#)
- [Cisco ISE Alarms, page 624](#)
- [Log Collection, page 635](#)
- [Live Authentications, page 636](#)
- [Global Search for Endpoints, page 638](#)
- [Session Trace for an Endpoint, page 639](#)
- [Authentication Summary Report, page 641](#)
- [Diagnostic Troubleshooting Tools, page 642](#)
- [TCP Dump Utility to Validate the Incoming Traffic, page 644](#)
- [Download Endpoint Statistical Data From Monitoring Nodes, page 648](#)
- [Obtaining Additional Troubleshooting Information, page 648](#)
- [Monitoring Database, page 653](#)

### Monitoring and Troubleshooting Service in Cisco ISE

The Monitoring and troubleshooting service is a comprehensive identity solution for all Cisco ISE run-time services and uses the following components:

- **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.

## 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.

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.

## Network Privilege Framework

The dashboard shows the activity on the Network Privilege Framework (NPF), and provides detailed information on the various components.

The NPF is composed of the three tiers outlined in the following table:

**Table 43: NPF Tiers**

Tier	Specifications
1	Access control based on identity using 802.1x, MAC authentication bypass (MAB), the Cisco ISE Profiler service
2	Access control based on identity using 802.1x, MAB, Profiler, guest provisioning of the Network Admission Control (NAC) manager, central web authentication
3	Access control based on identity and posture using 802.1x, MAB, Profiler, guest provisioning of the NAC manager, central web authentication

NPF authentication and authorization generates a flow of events. The events from the different sources are then collected by Cisco ISE monitoring and troubleshooting tools and summarized. You can view the authentication and authorization results on the dashboard or choose to run any number of reports.

## NPF Event Flow Process

The NPF authentication and authorization event flow uses the process described in the following table:

Process Stage	Description
1	NAD performs an authorization or flex authorization.
2	An unknown agentless identity is profiled with web authorization.
3	RADIUS server authenticates and authorizes the identity.
4	Authorization is provisioned for the identity at the port.
5	Unauthorized endpoint traffic is dropped.

## 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.

## 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.

## Network Process Status

You can view process status for the network from the Cisco ISE dashboard using the System Summary dashlet. For example, when processes like the application server or database fail, an alarm is generated and you can view the results using the System Summary dashlet.

The color of the system status icon indicates the health of your system:

- Green = Healthy
- Yellow = Warning
- Red = Critical
- Gray = No information

## Monitor Network Process Status

- 
- Step 1** Go to the Cisco ISE **Dashboard**.
- Step 2** Expand the **System Summary** dashlet. A detailed real-time report appears.
- Step 3** Review the following information for the processes that are running on the network:
- Name of the process
  - CPU and memory utilization
  - Time since process started running
- 

## Network Authentications

You can view the passed and failed network authentications from the Authentications dashlet. It provides data on the user or type of device, location, and the identity group to which the user or device belongs. The sparklines along the top of the dashlet represent distribution over the last 24 hours and the last 60 minutes.

## Monitor Network Authentications

- 
- Step 1** Go to the Cisco ISE **Dashboard**.
- Step 2** Expand the **Authentications** dashlet.  
A detailed real-time report appears.
- Step 3** Review the information for the users or devices that are authenticated on the network.
- Step 4** Expand the data categories for more information.
- 

## Profiler Activity and Profiled Endpoints

The Profiled Endpoint dashlet focuses on the endpoints on the network that have matched profiles, providing profile data for each endpoint. For example, the statistics allow you to determine the type of device, its location, and its IP address. The sparklines along the top of the dashlet represent endpoint activity over the last 24 hours and last 60 minutes.

The Profiled Endpoint dashlet represents the total number of endpoints that have been profiled on the network for the last 24 hours, including those that are unknown. It is not a representation of how many endpoints are currently active on the network. Sparkline metrics at the top of the dashlet show time specific values for the last 24 hours and 60 minutes.

## Determine Profiler Activity and Profiled Endpoints

- 
- Step 1** Go to the Cisco ISE **Dashboard**.
- Step 2** In the **Profiler Activity** 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 **Profiler Activity** dashlet. A detailed real-time report appears.
- 

## 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:

Test result: Failure: FeedService test connection failed : Feed Service unavailable : SocketTimeoutException invoking https://ise.cisco.com:8443/feedserver/feed/serverinfo: sun.security.validator.ValidatorException:PKIX path building failed: Sun.security.provider.certpath.SunCertPathBuilderException **Unable to find valid certification path to requested target**

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.
- 

## 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 a minimum duration of two hours. During the time that the event re-occurs, depending up on the trigger, it may take up to three hours for the alarms to re-appear.

The following table lists all the Cisco ISE alarms, descriptions and their resolution.

**Table 44: Cisco ISE Alarms**

Alarm Name	Alarm Description	Alarm Resolution
Administrative and Operational Audit Management		
Administrator account Locked/Disabled	Administrator account is locked or disabled due to password expiration or incorrect login attempts. For more details, refer to the administrator password policy.	Administrator password can be reset by another administrator using the GUI or CLI.

Alarm Name	Alarm Description	Alarm Resolution
Backup Failed	The ISE backup operation failed.	Check the network connectivity between Cisco ISE and the repository. Ensure that: <ul style="list-style-type: none"> <li>• The credentials used for the repository is correct.</li> <li>• There is sufficient disk space in the repository.</li> <li>• The repository user has write privileges.</li> </ul>
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.
Certificate Expiration	This certificate will expire soon. When it expires, Cisco ISE may fail to establish secure communication with clients.	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.
Certificate Revoked	Administrator has revoked the certificate issued to an Endpoint by the Internal CA.	Go through the BYOD flow from the beginning to be provisioned with a new certificate.
Certificate Provisioning Initialization Error	Certificate provisioning initialization failed	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.

Alarm Name	Alarm Description	Alarm Resolution
Certificate Replication Failed	Certificate replication to secondary node failed	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.
Certificate Replication Temporarily Failed	Certificate replication to secondary node temporarily failed	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.
Certificate Expired	This certificate has expired. Cisco ISE may fail to establish secure communication with clients. Node-to-node communication may also be affected.	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.
Certificate Request Forwarding Failed	Certificate request forwarding failed.	Make sure that the certification request coming in matches with attributes from the sender.
Configuration Changed	Cisco ISE configuration is updated. This alarm is not triggered for any configuration change in users and endpoints.	Check if the configuration change is expected.
CRL Retrieval Failed	Unable to retrieve CRL from the server. This could occur if the specified CRL is unavailable.	Ensure that the download URL is correct and is available for the service.
DNS Resolution Failure	DNS resolution failed on the node.	Check if the DNS server configured by the command <b>ip name-server</b> is reachable.  If you get the alarm as 'DNS Resolution failed for CNAME <hostname of the node>', then ensure that you create CNAME RR along with the A record for each Cisco ISE node.



Alarm Name	Alarm Description	Alarm Resolution
Firmware Update Required	A firmware update is required on this host.	Contact Cisco Technical Assistance Center to obtain firmware update
Insufficient Virtual Machine Resources	Virtual Machine (VM) resources such as CPU, RAM, Disk Space, or IOPS are insufficient on this host.	Ensure that a minimum requirements for the VM host, as specified in the Cisco ISE Hardware Installation Guide.
NTP Service Failure	The NTP service is down on this node.	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 <b>ntp server &lt;servername&gt;</b> CLI command to restart the NTP service and fix the time gap.
NTP Sync Failure	All the NTP servers configured on this node are unreachable.	Execute <b>show ntp</b> 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.
No Configuration Backup Scheduled	No Cisco ISE configuration backup is scheduled.	Create a schedule for configuration backup.
Operations DB Purge Failed	Unable to purge older data from the operations database. This could occur if M&T nodes are busy.	Check the Data Purging Audit report and ensure that the used_space is lesser than the threshold_space. Login to M&T nodes using CLI and perform the purge operation manually.
Profiler SNMP Request Failure	Either the SNMP request timed out or the SNMP community or user authentication data is incorrect.	Ensure that SNMP is running on the NAD and verify that SNMP configuration on Cisco ISE matches with NAD.
Replication Failed	The secondary node failed to consume the replicated message.	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.

Alarm Name	Alarm Description	Alarm Resolution
Restore Failed	Cisco ISE restore operation failed.	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 <b>reset-config</b> command from the CLI and restore the last known good backup.
Patch Failure	A patch process has failed on the server.	Re-install the patch process on the server.
Patch Success	A patch process has succeeded on the server.	-
External MDM Server API Version Mismatch	External MDM server API version does not match with what is configured in Cisco ISE.	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.
External MDM Server Connection Failure	Connection to the external MDM server failed.	Ensure that the MDM server is up and Cisco ISE-MDM API service is running on the MDM server.
External MDM Server Response Error	External MDM Server response error.	Ensure that the Cisco ISE-MDM API service is properly running on the MDM server.
Replication Stopped	ISE node could not replicate configuration data from the PAN.	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.
Endpoint certificates expired	Endpoint certificates were marked expired by daily scheduled job.	Please re-enroll the endpoint device to get a new endpoint certificate.
Endpoint certificates purged	Expired endpoint certificates were purged by daily scheduled job.	No action needed - this was an administrator-initiated cleanup operation.
Endpoints Purge Activities	Purge activities on endpoints for the past 24 hours. This alarm is triggered at mid-night.	Review the purge activities under <b>Operations &gt; Reports &gt; Endpoints and Users &gt; Endpoint Purge Activities</b>
Slow Replication Error	Slow or a stuck replication is detected .	Please verify that the node is reachable and part of the deployment.

Alarm Name	Alarm Description	Alarm Resolution
Slow Replication Info	Slow or a stuck replication is detected .	Please verify that the node is reachable and part of the deployment.
Slow Replication Warning	Slow or a stuck replication is detected .	Please verify that the node is reachable and part of the deployment.
PAN Auto Failover - Failover Failed	Promotion request to the Secondary administration node failed.	Please refer to the alarm details for further action.
PAN Auto Failover - Failover Triggered	Successfully triggered the failover of the Secondary Administration node to Primary role.	Wait for promotion of secondary PAN to complete and bring up the old primary PAN.
PAN Auto Failover - Health Check Inactivity	PAN did not receive the health check monitoring request from the designated monitoring node.	Please verify if the reported monitoring node is down or out-of-sync and trigger a manual sync if needed.
PAN Auto Failover - Invalid Health Check	Invalid health check monitoring request received for auto-failover.	Please verify if the health check monitoring node is out-of-sync and trigger a manual sync if needed.
PAN Auto Failover - Primary Administration Node Down	Primary Admin node is down or is not reachable from the monitoring node.	Bring up the PAN or wait for failover to happen.
PAN Auto Failover - Rejected Failover Attempt	Secondary administration node rejected the promotion request made by the health check monitor node.	Please refer to the alarm details for further action.
ISE Services		
AD Connector had to be restarted	AD Connector stopped unexpectedly and had to be restarted.	If this issue persists, contact the Cisco TAC for assistance.
Active Directory forest is unavailable	Active Directory forest GC (Global Catalog) is unavailable, and cannot be used for authentication, authorization and group and attribute retrieval.	Check DNS configuration, Kerberos configuration, error conditions, and network connectivity.
Authentication domain is unavailable	Authentication domain is unavailable, and cannot be used for authentication, authorization and group and attribute retrieval.	Check DNS configuration, Kerberos configuration, error conditions, and network connectivity.
ISE Authentication Inactivity	Cisco ISE policy service nodes are not receiving authentication requests from the network devices.	Check the ISE/NAD configuration. Check the network connectivity of the ISE/NAD infrastructure.

Alarm Name	Alarm Description	Alarm Resolution
ID Map. Authentication Inactivity	No User Authentication events were collected by the Identity Mapping service in the last 15 minutes.	If this is a time when User Authentications are expected (e.g. work hours), then check the connection to Active Directory domain controllers.
COA Failed	Network device has denied the Change of Authorization (CoA) request issued by Cisco ISE policy service nodes.	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.
Configured nameserver is down	Configured nameserver is down or unavailable.	Check DNS configuration and network connectivity.
Supplicant Stopped Responding	Cisco ISE sent last message to the client 120 seconds ago but there is no response from the client.	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.
Excessive Authentication Attempts	Cisco ISE policy service nodes are experiencing higher than expected rate of authentications.	<p>Check the re-auth timer in the network devices. Check the network connectivity of the Cisco ISE infrastructure.</p> <p>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.</p>
Excessive Failed Attempts	Cisco ISE policy service nodes are experiencing higher than expected rate of failed authentications.	<p>Check the authentication steps to identify the root cause. Check the Cisco ISE/NAD configuration for identity and secret mismatch.</p> <p>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.</p>

<b>Alarm Name</b>	<b>Alarm Description</b>	<b>Alarm Resolution</b>
AD: Machine TGT refresh failed	ISE server TGT (Ticket Granting Ticket) refresh has failed; it is used for AD connectivity and services.	Check that the ISE machine account exists and is valid. Also check for possible clock skew, replication, Kerberos configuration and/or network errors.
AD: ISE account password update failed	ISE server has failed to update it's AD machine account password.	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.
Joined domain is unavailable	Joined domain is unavailable, and cannot be used for authentication, authorization and group and attribute retrieval.	Check DNS configuration, Kerberos configuration, error conditions, and network connectivity.
Identity Store Unavailable	Cisco ISE policy service nodes are unable to reach the configured identity stores.	Check the network connectivity between Cisco ISE and identity store.
Misconfigured Network Device Detected	Cisco ISE has detected too many RADIUS accounting information from NAS	Too many duplicate RADIUS accounting information has been sent to ISE from NAS. Configure NAS with accurate accounting frequency.
Misconfigured Supplicant Detected	Cisco ISE has detected mis-configured supplicant on the network	Ensure that the configuration on Supplicant is correct.
No Accounting Start	Cisco ISE policy service nodes have authorized a session but did not receive accounting start from the network device.	Ensure that RADIUS accounting is configured on the network device. Check the network device configuration for local authorization.
Unknown NAD	Cisco ISE policy service nodes are receiving authentication requests from a network device that is not configured in Cisco ISE.	Check if the network device is a genuine request and add it to the configuration. Ensure that the secret matches.
SGACL Drops	Secure Group Access (SGACL) drops occurred. This occurs if a Trustsec capable device drops packets due to SGACL policy violations.	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.

Alarm Name	Alarm Description	Alarm Resolution
RADIUS Request Dropped	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.	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.
EAP Session Allocation Failed	A RADIUS request was dropped due to reaching EAP sessions limit. This condition can be caused by too many parallel EAP authentication requests.	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.
RADIUS Context Allocation Failed	A RADIUS request was dropped due to system overload. This condition can be caused by too many parallel authentication requests.	Wait for a few seconds before invoking a new RADIUS request. If system overload continues to occur, try restarting the ISE Server.
System Health		
High Disk I/O Utilization	Cisco ISE system is experiencing high disk I/O utilization.	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.
High Disk Space Utilization	Cisco ISE system is experiencing high disk space utilization.	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.
High Load Average	Cisco ISE system is experiencing high load average.	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.

Alarm Name	Alarm Description	Alarm Resolution
High Memory Utilization	Cisco ISE system is experiencing high memory utilization.	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.
High Operations DB Usage	Cisco ISE monitoring nodes are experiencing higher volume of syslog data than expected.	Check and reduce the purge configuration window for the operations data.
High Authentication Latency	Cisco ISE system is experiencing high authentication latency.	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.
Health Status Unavailable	The monitoring node has not received health status from the Cisco ISE node.	Ensure that Cisco ISE nodes are up and running. Ensure that Cisco ISE nodes are able to communicate with the monitoring nodes.
Process Down	One of the Cisco ISE processes is not running.	Restart the Cisco ISE application.
Profiler Queue Size Limit Reached	The ISE Profiler queue size limit has been reached. Events received after reaching the queue size limit will be dropped.	Check if the system has sufficient resources, and ensure EndPoint attribute filter is enabled.
OCSP Transaction Threshold Reached	The OCSP transaction threshold has been reached. This alarm is triggered when internal OCSP service reach high volume traffic.	Please check if the system has sufficient resources.
Licensing		
License About to Expire	License installed on the Cisco ISE nodes are about to expire.	View the Licencing page in Cisco ISE to view the license usage.
License Expired	License installed on the Cisco ISE nodes has expired.	Contact Cisco Accounts team to purchase new licenses.
License Violation	Cisco ISE nodes have detected that you are exceeding or about to exceed the allowed license count.	Contact Cisco Accounts team to purchase additional licenses.
System Error		

Alarm Name	Alarm Description	Alarm Resolution
Log Collection Error	Cisco ISE monitoring collector process is unable to persist the audit logs generated from the policy service nodes.	This will not impact the actual functionality of the Policy Service nodes. Contact TAC for further resolution.
Scheduled Report Export Failure	Unable to copy the exported report (CSV file) to configured repository.	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.

Alarms are not triggered when you add users or endpoints to Cisco ISE.

## Add Custom Alarms

System-defined alarms are listed in the Alarms Settings page. You can add additional alarms based on your requirements.

You can edit or delete the custom alarms. System-defined alarms cannot be deleted. But you can edit these alarms.

To add an alarm:

- 
- Step 1** Choose **Administration > System > Settings > Alarm Settings**.
  - Step 2** Click **Add** under the **Alarm Configuration** tab.
  - Step 3** Enter the required details.  
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.



## 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 > Authentications**.
  - 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 text box. 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 > Authentications**.

**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:

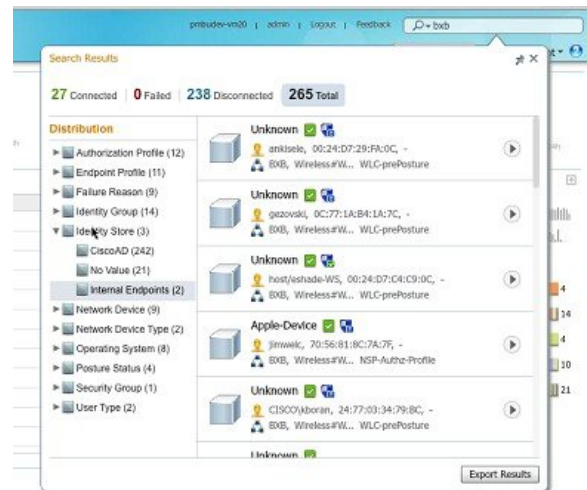
- User name
- MAC Address
- IP Address
- Authorization Profile
- Endpoint Profile
- Failure Reason
- Identity Group
- Identity Store
- Network Device name
- Network Device Type
- Operating System
- Posture Status
- Location
- Security Group
- User Type

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 51: 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
- Authentication details
- Accounting details
- Posture details
- Profiler details
- Client Provisioning details
- Guest accounting and activity

## Session Trace for an Endpoint

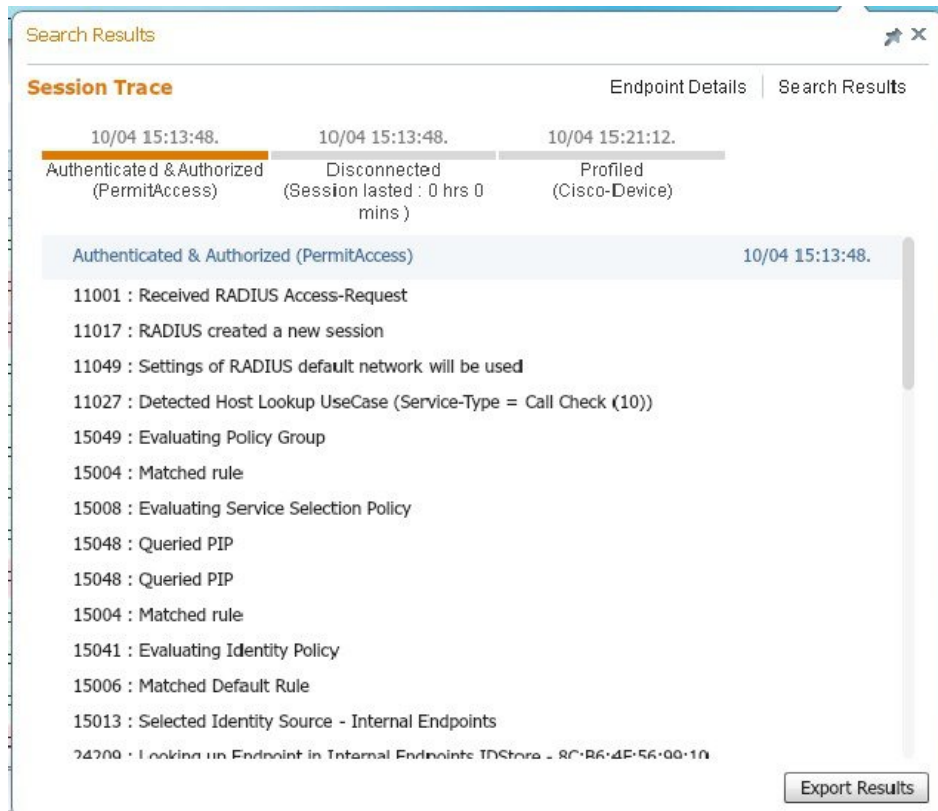
You can use the global search box available at the top of the Cisco ISE home page to get session information for a particular endpoint. When you search with a criteria, you get a list of endpoints. Click on any of these endpoints to see the session trace information for that endpoint. The following figure 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 52: 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.

**Figure 53: Endpoint Details**

Name	Value
Source Timestamp	2012-11-07 10:54:40.688
Received Timestamp	2012-11-07 10:54:40.689
Policy Server	ise230
Event	80002 Profiler EndPoint profiling event occurred
Mac Address	00:0C:29:95:A5:C1
Endpoint Policy	WindowsXP-Workstation
Static Assignment	
Source	
Oui	VMware, Inc.
Hostname	
Property	port=9,StaticAssignment=false,VlanName=VLAN0030,ifOperStatus=1,cafSessionAuthorizedBy=Authentication Server;ifIndex=10109,ifDescr=GigabitEthernet1/0/9,cafSessionAuthUserName=00-0C-29-95-A5-C1,cafSessionDomain=2,BYODRegistration=Unknown,EndPointPolicyID=a5f92810-be86-11e1-ba69-0050568e002b,FirstCollection=1352205183395,TimeToProfile=70.1,astNmapScanTime=0,cafSessionStatus

## 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 cleaned after seven days.

## 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.
- 

## 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** Choose **Operations > Troubleshoot > Diagnostic Tools > General Tools > Execute Network Device Command**.
  - 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

- 
- Step 1** Choose **Operations > Troubleshoot > Diagnostic Tools > General Tools > Posture Troubleshooting**.
- Step 2** Enter the information in the appropriate fields.
- Step 3** Click **Search**.
- Step 4** To find an explanation and determine a resolution for an event, select the event in the list and click **Troubleshoot**.
- 

## 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.

## 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.
- You must have Adobe Flash Player installed on the Cisco ISE administration node to be able to view the tcpdump file.

- 
- 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. Inline Posture nodes are not supported.
- 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. Standard tcpdump filter expressions are supported, such as the following:  
host 10.0.2.1 and port 1812
- 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.
- 


**Note**

Cisco ISE does not support frames greater than 1500 MTU (jumbo frames).

## 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:

Process Stage	Description
1	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.
2	Checks the egress policy that is configured in Cisco ISE and obtains the ACLs for each source and destination SGT pair.
3	Compares the SGACL policy that is obtained from the network device with the SGACL policy that is obtained from Cisco ISE.
4	Displays the source and destination SGT pair if there is a mismatch. Also, displays the matching entries as additional information.

## 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**.
  - Step 5** Click **Show Results Summary** to view the diagnosis and resolution steps.
- 

### 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.

**Note**

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.

## 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 650](#).

- 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 650](#).

## 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.

### 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** Enter and re-enter the encryption key for the support bundle.
- Step 6** Click **Create Support Bundle**.
- Step 7** 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.

## 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.
- 

## Cisco ISE Components and the Corresponding Debug Logs

*Table 45: Components and Corresponding Debug Logs*

Component	Debug Log
Active Directory	ad_agent.log
Cache Tracker	tracking.log
Entity Definition Framework (EDF)	edf.log
JMS	ise-psc.log
License	ise-psc.log
Notification Tracker	tracking.log
Replication-Deployment	replication.log
Replication-JGroup	replication.log
Replication Tracker	tracking.log
RuleEngine-Attributes	ise-psc.log
RuleEngine-Policy-IDGroups	ise-psc.log
accessfilter	ise-psc.log
admin-infra	ise-psc.log
boot-strap wizard	ise-psc.log
cisco-mnt	ise-psc.log
client	ise-psc.log
cpm-clustering	ise-psc.log
cpm-mnt	ise-psc.log
epm-pdp	ise-psc.log
epm-pip	ise-psc.log
epsanc	ise-psc.log
anc	ise-psc.log

<b>Component</b>	<b>Debug Log</b>
ers	ise-psc.log
guest	ise-psc.log
guestauth	ise-psc.log
guestportal	ise-psc.log
identitystore-AD	ise-psc.log
infrastructure	ise-psc.log
mdm	ise-psc.log
mdm-pip	ise-psc.log
mnt-alarm	alarms.log
mnt-report	reports.log
mydevices	ise-psc.log
nsf	ise-psc.log
nsf-session	ise-psc.log
org-apache	ise-psc.log
org-apache-cxf	ise-psc.log
org-apache-digester	ise-psc.log
posture	ise-psc.log
profiler	profiler.log
provisioning	ise-psc.log
prrt-JNI	prrt-management.log
runtime-AAA	prrt-management.log
runtime-config	prrt-management.log
runtime-logging	prrt-management.log
sponsorportal	ise-psc.log
swiss	ise-psc.log

## 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** 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
  - catalina.log—Provides third-party 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:

### 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.

## 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.

## Purge Older Monitoring Data

### Before You Begin

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

- 
- Step 1** Choose **Administration > System > Maintenance > Data Purging**.
- Step 2** Specify the time period in months, for which the data will be retained. All the data prior to the specified time period will be purged. For this option, each month consists of 30 days. The default of three months equals 90 days.  
**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.
- Step 3** Click **Submit**.
- Step 4** Verify the success of the data purge by viewing the Data Purging Audit report.
-

**What to Do Next**

Cisco ISE Log Collection

Perform an On-demand Backup





## CHAPTER 26

# Reports

---

- [Cisco ISE Reports, page 657](#)
- [Run and View Reports, page 658](#)
- [Reports Navigation, page 658](#)
- [Export Reports, page 658](#)
- [Schedule and Save Cisco ISE Reports, page 659](#)
- [Add Favorite Reports, page 660](#)
- [Cisco ISE Active RADIUS Sessions, page 660](#)
- [Available Reports, page 662](#)

## 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 are grouped into logical categories with information related to authentication, session traffic, device administration, configuration and administration, and troubleshooting.

## Run and View Reports

This section describes how to run, view, and navigate reports using Reports View. You can specify time increments over which to display data in a report.

- 
- Step 1** Choose **Operations > Reports > ISE Reports**.
  - Step 2** Click a report from the **report** categories available.
  - Step 3** 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 4** Enter an appropriate value for the filters.
  - Step 5** Run the report.
- 

## 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 to an 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.

You cannot export the following reports:

- Authentication Summary
- Health Summary
- RBACL Drop Summary
- 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 Administration Node (PAN).

---

- 
- Step 1** Run a report, as described in the Running and Viewing Reports section.
- Step 2** Click **Export** in the top right-hand corner of the report summary page.
- Step 3** Specify the data columns that you want to export.
- Step 4** Choose a repository from the drop-down list.
- Step 5** Click **Export** .
- 

## Schedule and Save Cisco ISE Reports

You can customize a report and save the changes as a new report, or restore the default report settings.

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.

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 **Save As** in the top right-hand corner of the report summary page.
- Step 3** Choose **Report** or **Scheduled Report**.
- Step 4** Enter the required details in the dialog box.
- Step 5** 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.

## Add Favorite Reports

You can add preconfigured system reports to your favorites list, as well as reports that you have customized.

You can add reports that you use frequently to a list of favorites to make them easier to find, similar to how you bookmark favorite websites in a browser. You can view and edit the parameters of your favorite reports, and then save the customized reports for reuse.




---

**Note** Every administrator account is assigned one or more administrative roles. Depending on the roles that are assigned to your account, you may not be able to perform the tasks that are described in this section.

---



---

**Step 1** Run a report, as described in Running and Viewing Reports section.

**Step 2** Click **Favorite** in the top right-hand corner of the report summary page. The report appears in your Favorites list.

**Note** You can add preconfigured system reports to your favorites list only from the PAN.

---

## 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.

---

## 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 > Authentications**.

**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:

**Note** For Inline Posture nodes and where wireless LAN controllers (WLC) are in use, only two options are available: Session reauthentication and Session termination.

- **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.

**Table 46: Available Reports**

Report Name	Description	Logging Category
Auth Services Status		
AAA Diagnostics	The AAA Diagnostics report provides details of all network sessions between Cisco ISE and users. If users cannot access the network, you can review this report to identify trends and identify whether the issue is isolated to a particular user or indicative of a more widespread problem.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select these logging categories: Policy Diagnostics, Identity Stores Diagnostics, Authentication Flow Diagnostics, and RADIUS Diagnostics.
RADIUS Authentications	The RADIUS Authentications report enables you to review the history of authentication failures and successes. If users cannot access the network, you can review the details in this report to identify possible causes.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select these logging categories: Passed Authentications and Failed Attempts.
RADIUS Errors	<p>The RADIUS Errors report enables you to check for RADIUS Requests Dropped (authentication/accounting requests discarded from unknown Network Access Device), EAP connection time outs and unknown NADs.</p> <p><b>Note</b> Sometimes ISE will silently drop the Accounting Stop request of an endpoint if user authentication is in progress. However, ISE starts acknowledging all accounting requests once the user authentication is completed.</p>	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select Failed Attempts.

Report Name	Description	Logging Category
RADIUS Accounting	The RADIUS Accounting report identifies how long users have been on the network. If users are losing network access, you can use this report to identify whether Cisco ISE is the cause of the network connectivity issues.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select RADIUS Accounting.
Authentication Summary	<p>The Authentication Summary report is based on the RADIUS authentications. It enables you to identify the most common authentications and the reason for any authentication failures. For example, if one Cisco ISE server is handling significantly more authentications than others, you might want to reassign users to different Cisco ISE servers to better balance the load.</p> <p><b>Note</b> 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.</p>	—

Report Name	Description	Logging Category
OCSP Monitoring	The OCSP Monitoring Report specifies the status of the Online Certificate Status Protocol (OCSP) services. It identifies whether Cisco ISE can successfully contact a certificate server and provides certificate status auditing. Provides a summary of all the OCSP certificate validation operations performed by Cisco ISE. It retrieves information related to the good and revoked primary and secondary certificates from the OCSP server. Cisco ISE caches the responses and utilizes them for generating subsequent OCSP Monitoring Reports. In the event the cache is cleared, it retrieves information from the OCSP server.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select System Diagnostics.
AD Connector Operations	The AD Connector Operations report provides log of operations performed by AD Connector such as Cisco ISE Server password refresh, Kerberos tickets management, DNS queries, DC discovery, LDAP, and RPC Connections management, etc.  If some AD failures are encountered, you can review the details in this report to identify the possible causes.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select AD Connector.
Identity Mapping	The Identity Mapping report enables you to monitor the state of WMI connection to the domain controller and gather statistics related to it (such as amount of notifications received, amount of user login/logouts per second etc.)	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select Identity Mapping.
Deployment Status		

Report Name	Description	Logging Category
Administrator Logins	The Administrator Logins report provides information about all GUI-based administrator login events as well as successful CLI login events.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select Administrative and Operational audit.
Internal Administrator Summary	The Internal Administrator Summary report enables you to verify the entitlement of administrator users. From this report, you can also access the Administrator Logins and Change Configuration Audit reports, which enables you to view these details for each administrator.	—
Change Configuration Audit	The Change Configuration Audit report provides details about configuration changes within a specified time period. If you need to troubleshoot a feature, this report can help you determine if a recent configuration change contributed to the problem.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select Administrative and Operational audit.
Secure Communications Audit	The Secure Communications Audit report provides auditing details about security-related events in Cisco ISE Admin CLI, which includes authentication failures, possible break-in attempts, SSH logins, failed passwords, SSH logouts, invalid user accounts, and so on.	—
Operations Audit	The Operations Audit report provides details about any operational changes, such as: running backups, registering a Cisco ISE node, or restarting an application.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select Administrative and Operational audit.

Report Name	Description	Logging Category
System Diagnostics	<p>The System Diagnostic report provides details about the status of the Cisco ISE nodes. If a Cisco ISE node is unable to register, you can review this report to troubleshoot the issue.</p> <p>This report requires that you first enable several diagnostic logging categories. Collecting these logs can negatively impact Cisco ISE performance. So, these categories are not enabled by default, and you should enable them just long enough to collect the data. Otherwise, they are automatically disabled after 30 minutes.</p>	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select these logging categories: Internal Operations Diagnostics, Distributed Management, Administrator Authentication and Authorization.
Health Summary	<p>The Health Summary report provides details similar to the Dashboard. However, the Dashboard only displays data for the past 24 hours, and you can review more historical data using this report.</p> <p>You can evaluate this data to see consistent patterns in data. For example, you would expect heavier CPU usage when most employees start their work days. If you see inconsistencies in these trends, you can identify potential problems.</p>	—



Report Name	Description	Logging Category
Network Device Session Status	<p>The Network Device Session Status Summary report enables you to display the switch configuration without logging into the switch directly.</p> <p>Cisco ISE accesses these details using an SNMP query and requires that your network devices are configured with SNMP v1/v2c.</p> <p>If a user is experiencing network issues, this report can help you identify if the issue is related to the switch configuration rather than with Cisco ISE.</p>	—
Data Purging Audit	<p>The Data Purging Audit report records when the logging data is purged.</p> <p>This report reflects two sources of data purging.</p> <p>At 4AM daily, Cisco ISE checks whether there are any logging files that meet the criteria you have set on the Administration &gt; Maintenance &gt; Data Purging page. If so, the files are deleted and recorded in this report.</p> <p>Additionally, Cisco ISE continually maintains a maximum of 80% used storage space for the log files. Every hour, Cisco ISE verifies this percentage and deletes the oldest data until it reaches the 80% threshold again. This information is also recorded in this report.</p>	—

Report Name	Description	Logging Category
pxGrid Administrator Audit	<p>The pxGrid Administrator Audit report provides the details of the pxGrid administration actions such as client registration, client deregistration, client approval, topic creation, topic deletion, publisher-subscriber addition, and publisher-subscriber deletion on the PAN.</p> <p>Every record has the administrator name who has performed the action on the node.</p> <p>You can filter the pxGrid Administrator Audit report based on the administrator and message criteria.</p>	—
Misconfigured Supplicants	<p>The Misconfigured Supplicants report provides a list of mis-configured supplicants along with the statistics due to failed attempts that are performed by a specific supplicant. If you have taken corrective actions and fix the mis-configured supplicant, the report displays fixed acknowledgment in the report.</p> <p><b>Note</b> RADIUS Suppression should be enabled to run this report.</p>	—
Misconfigured NAS	<p>The Misconfigured NAS report provides information about NADs with inaccurate accounting frequency typically when sending accounting information frequently. If you have taken corrective actions and fix the mis-configured NADs, the report displays fixed acknowledgment in the report.</p> <p><b>Note</b> RADIUS Suppression should be enabled to run this report.</p>	—
Endpoints and Users		

Report Name	Description	Logging Category
Client Provisioning	The Client Provisioning report indicates the client provisioning agents applied to particular endpoints. You can use this report to verify the policies applied to each endpoint to verify whether the endpoints have been correctly provisioned.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select Posture and Client Provisioning Audit and Posture and Client Provisioning Diagnostics.
Current Active Sessions	The Current Active Sessions report enables you to export a report with details about who was currently on the network within a specified time period.  If a user isn't getting network access, you can see whether the session is authenticated or terminated or if there is another problem with the session.	—
Endpoint Protection Service Adaptive Network Control Audit	The Endpoint Protection Service Adaptive Network Control Audit report is based on the RADIUS accounting. It displays historical reporting of all network sessions for each endpoint.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select Passed Authentications and RADIUS Accounting.
External Mobile Device Management	The External Mobile Device Management report provides details about integration between Cisco ISE and the external Mobile Device Management (MDM) server.  You can use this report to see which endpoints have been provisioned by the MDM server without logging into the MDM server directly. It also displays information such as registration and MDM-compliance status.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select MDM.

Report Name	Description	Logging Category
Posture Detail Assessment	The Posture Detail Assessment report provides details about posture compliancy for a particular endpoint. If an endpoint previously had network access and then suddenly was unable to access the network, you can use this report to determine if a posture violation occurred.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select Posture and Client Provisioning Audit and Posture and Client Provisioning Diagnostics.
Profiled Endpoint Summary	The Profiled Endpoint Summary report provides profiling details about endpoints that are accessing the network.  <b>Note</b> For endpoints that do not register a session time, such as a Cisco IP-Phone, the term Not Applicable is shown in the Endpoint session time field.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select Profiler.
Endpoint Profile Changes	The Endpoint Profile Change report serves two purposes: <ul style="list-style-type: none"> <li>• Compares the profile changes for a particular endpoint to verify that the latest and most current profile has been applied.</li> <li>• Displays profile changes initiated by the profiler feed service (which is available with a Cisco ISE Plus license).</li> </ul>	—
Top Authorizations by Endpoint	The Top Authorization by Endpoint (MAC address) report displays how many times each endpoint MAC address was authorized by Cisco ISE to access the network.	Passed Authentications, Failed Attempts
Top Authorizations by User	The Top Authorization by User report displays how many times each user was authorized by Cisco ISE to access the network.	Passed Authentications, Failed Attempts

Report Name	Description	Logging Category
User Change Password Audit	The User Change Password Audit report displays verification about employee's password changes.	Administrative and Operational audit
Supplicant Provisioning	The Supplicant Provisioning report provides details about the supplicants provisioned to employee's personal devices.	Posture and Client Provisioning Audit
Registered Endpoints	The Registered Endpoints report displays all personal devices registered by employees.	—
Endpoints Purge Activities	The Endpoints Purge Activities report enables the user to review the history of endpoints purge activities. This report requires that the Profiler logging category is enabled. It is enabled by default.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select Profiler.
Guest Access Reports		
AUP Acceptance Status	The AUP Acceptance Status report provides details of AUP acceptances from all the Guest portals.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select Guest.
Sponsor Login and Audit	The Sponsor Login and Audit report provides details of guest users' login, add, delete, enable, suspend and update operations and the login activities of the sponsors at the sponsors portal.  If guest users are added in bulk, they are visible under the column 'Guest Users.' This column is hidden by default. On export, these bulk users are also present in the exported file.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select Guest.
My Devices Login and Audit	The My Devices Login and Audit report provides details about the login activities and the operations performed by the users on the devices in My Devices Portal.	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select My Devices.

Report Name	Description	Logging Category
Master Guest Report	<p>The Master Guest Report combines data from various Guest Access reports and enables you to export data from different reporting sources. The Master Guest report also provides details about the websites that guest users are visiting. You can use this report for security auditing purposes to demonstrate when guest users accessed the network and what they did on it.</p> <p>You must also enable HTTP inspection on the network access device (NAD) used for guest traffic. This information is sent back to Cisco ISE by the NAD.</p> <p>To check when the clients reach the maximum simultaneous sessions limit, from the Admin portal, choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and do the following:</p> <ol style="list-style-type: none"> <li><b>1</b> Increase the log level of "Authentication Flow Diagnostics" logging category from WARN to INFO.</li> <li><b>2</b> Change LogCollector Target from Available to Selected under the "Logging Category" of AAA Diagnostics.</li> </ol>	Choose <b>Administration &gt; System &gt; Logging &gt; Logging Categories</b> and select Passed Authentications.
Guest Accounting	The Guest Accounting report is a subset of the RADIUS Accounting report. All users assigned to the Activated Guest or Guest identity groups appear in this report.	—
TrustSec		

Report Name	Description	Logging Category
RBACL Drop Summary	<p>The RBACL Drop Summary report is specific to the TrustSec feature, which is available only with an Advanced Cisco ISE license.</p> <p>This report also requires that you configure the network devices to send NetFlow events for dropped events to Cisco ISE.</p> <p>If a user violates a particular policy or access, packets are dropped and indicated in this report.</p>	—
Top N RBACL Drops By User	<p>The Top N RBACL Drops By User report is specific to the TrustSec feature, which is available only with an Advanced Cisco ISE license.</p> <p>This report also requires that you configure the network devices to send NetFlow events for dropped events to Cisco ISE.</p> <p>This report displays policy violations (based on packet drops) by specific users.</p>	—







# PART VII

## Reference

- [Administration User Interface Reference, page 677](#)
- [Guest Access User Interface Reference, page 755](#)
- [Web Portals Customization Reference, page 789](#)
- [Policy User Interface Reference, page 807](#)
- [Operations User Interface Reference, page 851](#)
- [Network Access Flows, page 863](#)
- [Switch and Wireless LAN Controller Configuration Required to Support Cisco ISE Functions, page 871](#)
- [Supported Management Information Bases in Cisco ISE, page 883](#)





# CHAPTER 27

## Administration User Interface Reference

- [System Administration, page 677](#)
- [Identity Management, page 715](#)
- [Network Resources, page 729](#)
- [Device Portal Management, page 741](#)

### System Administration

#### Deployment Settings

The Deployment Nodes page enables you to configure Cisco ISE (Administration, Policy Service, and Monitoring) nodes and Inline Posture 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 and Inline Posture nodes in a deployment. The navigation path for this page is: **Administration** > **System** > **Deployment**.

Fields	Usage Guidelines
Hostname	Displays the hostname of the node.
Node Type	Displays the node type. It can be one of the following: <ul style="list-style-type: none"><li>• Cisco ISE (Administration, Policy Service, and Monitoring) nodes</li><li>• Inline Posture node</li></ul>
Personas	(Only appears if the node type is Cisco ISE) Lists the personas that an Cisco ISE node has assumed. For example, Administration, Policy Service.

Fields	Usage Guidelines
Role	<p>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:</p> <ul style="list-style-type: none"> <li>• PRI(A)—Refers to the Primary Administration Node (PAN)</li> <li>• SEC(A)—Refers to the Secondary Administration Node</li> <li>• PRI(M)—Refers to the Primary Monitoring Node</li> <li>• SEC(M)—Refers to the Secondary Monitoring Node</li> </ul>
Services	<p>(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:</p> <ul style="list-style-type: none"> <li>• Session</li> <li>• Profiling</li> <li>• All</li> </ul>
Node Status	<p>Indicates the status of each ISE node in a deployment for data replication.</p> <ul style="list-style-type: none"> <li>• Green (Connected)—Indicates that an ISE node, which is already registered in the deployment is in sync with the PAN.</li> <li>• Red (Disconnected)—Indicates that an ISE node is not reachable or is down or data replication is not happening.</li> <li>• Orange (In Progress)—Indicates that an ISE node is newly registered with the PAN or you have performed a manual sync operation or the ISE node is not in sync (out of sync) with the PAN.</li> </ul> <p>For more details, click the quick view icon for each ISE node in the Node Status column.</p>

## 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 47: General Node Settings**

Fields	Usage Guidelines
Hostname	Displays the hostname of the Cisco ISE node.
FQDN	Displays the fully qualified domain name of the Cisco ISE node. For example, ise1.cisco.com.
IP Address	Displays the IP address of the Cisco ISE node.

Fields	Usage Guidelines
Node Type	Displays the node type. Could be any one of the following: Identity Services Engine (ISE), Inline Posture Node
Personas	
Administration	<p>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.</p> <p>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</p> <p>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.</p>
Monitoring	<p>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 PAN, you must enable the Monitoring persona. After you register a secondary Monitoring node in your deployment, you can edit the 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.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• Primary—For the current node to be the primary Monitoring node.</li> <li>• Secondary—For the current node to be the secondary Monitoring node.</li> <li>• None—If you do not want the Monitoring nodes to assume the primary-secondary roles.</li> </ul> <p>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 &gt; System &gt; Logging &gt; Remote Logging Targets</p>

Fields	Usage Guidelines
Policy Service	<p>Check this check box to enable any one or all of the following services:</p> <ul style="list-style-type: none"> <li>• <b>Enable Session Services</b>—Check this check box 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.</li> </ul> <p>Choose &lt;none&gt; if you do not want this Policy Service node to be part of any group.</p> <p>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.</p> <p>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.</p> <p>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 <a href="#">Create a Policy Service Node Group</a>, on page 64 section for more details.</p> <ul style="list-style-type: none"> <li>• <b>Enable Profiling Service</b>—Check this check box 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.</li> </ul>
pxGrid	<p>Check this check box to enable the pxGrid services. 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.</p>

## 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 48: Profiling Node Settings**

Fields	Usage Guidelines
NetFlow	<p>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:</p> <ul style="list-style-type: none"> <li>• Interface—Choose the interface on the ISE node.</li> <li>• Port—Enter the NetFlow listener port number on which NetFlow exports are received from the routers. The default port is 9996.</li> </ul>
DHCP	<p>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:</p> <ul style="list-style-type: none"> <li>• Interface—Choose the interface on the ISE node.</li> <li>• Port—Enter the DHCP server UDP port number. The default port is 67.</li> </ul>
DHCP SPAN	<p>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.</p> <ul style="list-style-type: none"> <li>• Interface—Choose the interface on the ISE node.</li> </ul>
HTTP	<p>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.</p> <ul style="list-style-type: none"> <li>• Interface—Choose the interface on the ISE node.</li> </ul>
RADIUS	<p>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.</p>
Network Scan (NMAP)	<p>Check this box to enable the NMAP probe. You can also do a manual scan of a subnet in this panel.</p>
DNS	<p>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.</p> <p><b>Note</b> 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.</p>

Fields	Usage Guidelines
SNMP Query	<p>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.</p> <p><b>Note</b> 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.</p>
SNMP Trap	<p>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:</p> <ul style="list-style-type: none"> <li>• Link Trap Query—Check this check box to receive and interpret linkup and linkdown notifications received through the SNMP Trap.</li> <li>• MAC Trap Query—Check this check box to receive and interpret MAC notifications received through the SNMP Trap.</li> <li>• Interface—Choose an interface on the ISE node.</li> <li>• Port—Enter the UDP port of the host to use. The default port is 162.</li> </ul>

### Inline Posture Node Settings

The following table describes the fields on the Deployment Nodes List page for an Inline Posture node, which you can use to configure the Inline Posture nodes in your deployment. The navigation path for this page is: **Administration > System > Deployment > Inline Posture Node > Edit**.

**Table 49: Inline Posture Node Settings**

Fields	Usage Guidelines
<b>Basic Information</b>	
Time Sync Server	Enter the IP address of the primary, secondary, and tertiary time sync server.
DNS Server	Enter the IP address of the primary, secondary, and tertiary DNS server.
Trusted Interface (to protected network)	Enter the Management VLAN ID (all the other information is automatically populated for these options)
Untrusted Interface (to management network)	Enter the IP Address, Subnet Mask, Default Gateway, and Management VLAN ID for the untrusted interface.
<b>Deployment Modes</b>	



Fields	Usage Guidelines
Routed Mode	Choose this option for this node to provide router (hop in the wire) functionality for Inline Posture.
Bridged Mode	<p>Choose this option for this node to provide VLAN mapping functionality for the subnets to be managed by Inline Posture. After checking the Bridged Mode check box, enter the Untrusted Network and Trusted Network VLAN ID information. For VLAN mapping, you should also do the following:</p> <ul style="list-style-type: none"> <li>• Add a mapping for management traffic by entering the appropriate VLAN ID for the trusted and untrusted networks.</li> <li>• Add a mapping for client traffic by entering the appropriate VLAN ID for the trusted and untrusted networks.</li> </ul>
<b>Filters</b>	
MAC Address	Enter the MAC Address of the device on which to avoid policies. For security reasons, we recommend that you always include the IP address along with the MAC address in a MAC filter entry. Do not configure the MAC address in a MAC filter for a directly connected ASA VPN device without also entering the IP address. Without the addition of the optional IP address, VPN clients are allowed to bypass policy enforcement. This bypass happens because the VPN is a Layer 3 hop for clients, and the device uses its own MAC address as the source address to send packets along the network toward the Inline Posture node.
IP Address	Enter the IP Address of the device on which to avoid policies.
Description	Enter a description of the MAC Filter.
Subnet Address	Enter the subnet Address of the device on which to avoid policies.
Subnet Mask	Enter the subnet Mask of the device on which to avoid policies
Description	Enter a description of the Subnet Filter.
<b>RADIUS Config</b>	
Primary Server	<p>Enter the IP address, shared secret, timeout in seconds, and number of retries for the primary RADIUS server, usually the Policy Service node.</p> <p>The timeout and retry values should be based on the timeout and retries that you define on the client such as WLC or ASA. We recommend the following: <math>(IPN \text{ RADIUS Config Timeout} * \text{No. of Retries}) &lt; (\text{Client device's Timeout} * \text{No. of Retries})</math>. For example, on the primary and secondary servers, you can configure the timeout to be 5 seconds and the number of retries to be 1, and on the client, you can configure the timeout to be 5 seconds and the number of retries to be 3. So the timeout * no. of retries configured on the IPN server (<math>5*1=5</math>) is lesser than the value configured on the client (<math>5*3=15</math>)</p>

Fields	Usage Guidelines
Secondary Server	<p>Enter the IP address, shared secret, timeout in seconds, and number of retries for the secondary RADIUS server.</p> <p>The timeout and retry values should be based on the timeout and retries that you define on the client such as WLC or ASA. We recommend the following: (IPN RADIUS Config Timeout * No. of Retries) &lt; (Client device's Timeout * No. of Retries). For example, on the primary and secondary servers, you can configure the timeout to be 5 seconds and the number of retries to be 1, and on the client, you can configure the timeout to be 5 seconds and the number of retries to be 3. So the timeout * no. of retries configured on the IPN server (5*1=5) is lesser than the value configured on the client (5*3=15)</p>
Client	<p>Enter the IP address, shared secret, timeout in seconds, and number of retries for the device that requests access on behalf of clients, WLC or VPN.</p> <p><b>Note</b> WLC roaming is not supported in Cisco ISE, Release 1.1.1.</p>
Enable KeyWrap	<p>Check this check box and specify the following Authentication Settings:</p> <ul style="list-style-type: none"> <li>• Key Encryption Key</li> <li>• Message Authenticator Code Key</li> <li>• Key Input Format: ASCII or Hexidecimal</li> </ul> <p>Deployments that utilize wireless LAN technology require secure transmission from a RADIUS server to a network access point. KeyWrap attributes provide stronger protection and more flexibility.</p>
<p><b>Failover</b> Displays only if you have deployed an Inline Posture high availability pair.</p>	

Fields	Usage Guidelines
HA Peer Node	<p>Choose the <b>HA Peer Node</b> from the drop-down list. A list of eligible standalone Inline Posture nodes appear from which to choose. The secondary node syncs to the primary node.</p> <ul style="list-style-type: none"> <li>• Replication Status—(Only appears for secondary nodes) Indicates whether incremental replication from the primary node to the secondary node is complete or not. You will see one of the following states: <ul style="list-style-type: none"> <li>◦ Failed—Incremental database replication has failed.</li> <li>◦ In-Progress—Incremental database replication is currently in progress.</li> <li>◦ Complete—Incremental database replication is complete. Not Applicable—Displayed if the Cisco ISE node is a standalone or primary node.</li> <li>◦ Not Applicable—Displayed if the Cisco ISE node is a standalone or primary node.</li> </ul> </li> <li>• Sync Status—(Only appears for secondary Cisco ISE nodes) Indicates whether replication from the primary node to the secondary node is complete or not. A replication happens when a node is registered as secondary or when you click Syncup to force a replication. You will see one of the following states: <ul style="list-style-type: none"> <li>◦ Sync Completed—Full database replication is complete.</li> <li>◦ Sync in Progress—Database replication is currently in progress.</li> <li>◦ Out of Sync—Database was down when the secondary node was registered with the primary Cisco ISE node.</li> <li>◦ Not Applicable—Displayed if the Cisco ISE node is a standalone node.</li> </ul> </li> </ul>
Service IP (Trusted)	Enter the Trusted Service IP address (eth0) for the traffic interface of the primary node.
Service IP (Untrusted)	Enter the Untrusted Service IP address (eth1) for the traffic interface of the primary node. In the bridged mode, the service IP address is the same for both trusted and untrusted networks.
Link Detect (Trusted)	Enter the IP address (optional, but recommended as a best practice) for the Link-Detect system for the trusted and untrusted sides. This address is usually the IP address of the Policy Service node, because both the active and standby nodes should always be able to reach the Policy Service node.
Link Detect (Untrusted)	Enter the IP address for the Link-Detect system for the untrusted side.

Fields	Usage Guidelines
Link Detect Timeout	Enter a Link-Detect Timeout value. The default value of 30 seconds is recommended. However, there is no maximum value. Link-detect ensures that the Inline Posture node maintains communication with the Policy Service node. If the active node does not receive notification (ping) from the Policy Service node at the specified intervals, the active node fails over to the standby node.
Heart Beat Timeout	Enter a Heart Beat Timeout value. The default value of 30 seconds is recommended. However, there is no maximum value. The heartbeat is a message that is sent between the two Inline Posture nodes at specified intervals. The heartbeat happens on eth2 and eth3 interfaces. If the heartbeat stops or does not receive a response in the allotted time, failover occurs.
Syncup Peer Node	If the sync status for any secondary node is out of sync, click Syncup Peer Node to force a full database replication.  <b>Note</b> You must use the Syncup option to force a full replication if the Sync Status is Out of Sync or the Replication Status is Failed.

## Certificate Store Settings

The Certificate Store page enables you to configure certificates in Cisco ISE that can be used for authentication.

### Endpoint Certificate Overview Page

The following table describes the fields on the Certificate Management Overview 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.

Fields	Usage Guidelines
Node Name	Name of the Policy Service node (PSN) that issued the certificate.
Endpoint Certificates Issued	Number of endpoint certificates issued by the PSN node.
Endpoint Certificates Revoked	Number of revoked endpoint certificates (certificates that were issued by the PSN node).
Endpoint Certificates Requests	Number of certificate-based authentication requests processed by the PSN node.
Endpoint Certificates Failed	Number of failed authentication requests processed by the PSN node.

## 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.

Fields	Usage Guidelines
Select Node	(Required) The node for which you want to generate the system certificate.
Common Name (CN)	(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.
Organizational Unit (OU)	Organizational Unit name. For example, Engineering.
Organization (O)	Organization name. For example, Cisco.
City (L)	(Do not abbreviate) City name. For example, San Jose.
State (ST)	(Do not abbreviate) State name. For example, California.
Country (C)	Country name. You must enter the two-letter ISO country code. For example, US.
Subject Alternative Name (SAN)	An IP address or DNS name that is associated with the certificate.
Key Length	Choose 2048 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.
Expiration TTL	Specify the number of days after which the certificate will expire.
Friendly Name	Enter a friendly name for the certificate. If you do not specify a name, Cisco ISE automatically creates a name in the format <common name> # <issuer> # <nnnnn> where <nnnnn> is a unique five-digit number.
Allow Wildcard Certificates	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.

Fields	Usage Guidelines
Usage	Choose the service for which this system certificate should be used: <ul style="list-style-type: none"> <li>• Admin—Server certificate used to secure communication with the Admin portal and between ISE nodes in a deployment</li> <li>• EAP Authentication—Server certificate used for authentications that use the EAP protocol for SSL/TLS tunneling</li> <li>• pxGrid—Client and server certificate to secure communication between the pxGrid client and server</li> <li>• Portal—Server certificate used to secure communication with all Cisco ISE web portals</li> </ul>

### 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 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 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.**

Field	Usage Guidelines
Certificate(s) will be used for	

Field	Usage Guidelines
	<p>Choose the service for which you are going to use the certificate:</p> <p><b>Cisco ISE Identity Certificates</b></p> <ul style="list-style-type: none"> <li>• <b>Multi-Use</b>—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: <ul style="list-style-type: none"> <li>◦ Key Usage: Digital Signature (Signing)</li> <li>◦ 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)</li> </ul> </li> <li>• <b>Admin</b>—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: <ul style="list-style-type: none"> <li>◦ Key Usage: Digital Signature (Signing)</li> <li>◦ Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)</li> </ul> </li> <li>• <b>EAP Authentication</b>—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: <ul style="list-style-type: none"> <li>◦ Key Usage: Digital Signature (Signing)</li> <li>◦ Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)</li> </ul> </li> <li>• <b>Portal</b>—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: <ul style="list-style-type: none"> <li>◦ Key Usage: Digital Signature (Signing)</li> <li>◦ Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1)</li> </ul> </li> <li>• <b>pxGrid</b>—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: <ul style="list-style-type: none"> <li>◦ Key Usage: Digital Signature (Signing)</li> <li>◦ 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)</li> </ul> </li> </ul> <p><b>Cisco ISE Certificate Authority Certificates</b></p> <ul style="list-style-type: none"> <li>• <b>ISE Root CA</b>—(Applicable only for the internal CA service ) Used for regenerating the entire internal CA certificate chain including the root CA on</li> </ul>



Field	Usage Guidelines
	<p>the PAN and subordinate CAs on the PSNs.</p> <ul style="list-style-type: none"> <li>• 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 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: <ul style="list-style-type: none"> <li>◦ Basic Constraints: Critical, Is a Certificate Authority</li> <li>◦ Key Usage: Certificate Signing, Digital Signature</li> <li>◦ Extended Key Usage: OCSP Signing (1.3.6.1.5.5.7.3.9)</li> </ul> </li> <li>• 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.</li> </ul>
Allow Wildcard Certificates	Check this check box to use a wildcard character (*) 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 (*) 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.
Generate CSRs for these Nodes	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.
Common Name (CN)	By default, the common name is the FQDN of the ISE node for which you are generating the CSR. \$FQDN\$ 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.
Organizational Unit (OU)	Organizational Unit name. For example, Engineering.
Organization (O)	Organization name. For example, Cisco.
City (L)	(Do not abbreviate) City name. For example, San Jose.
State (ST)	(Do not abbreviate) State name. For example, California.
Country (C)	Country name. You must enter the two-letter ISO country code. For example, US.

Field	Usage Guidelines
Subject Alternative Name (SAN)	<p>Available options for SAN include:</p> <ul style="list-style-type: none"> <li>• DNS Name—If you choose the DNS name, enter the fully qualified domain name of the ISE node. If you have enabled the Allow Wildcard Certificates option, specify the wildcard notation (an asterisk and a period before the domain name). For example, *.amer.example.com.</li> <li>• IP Address—IP address of the ISE node to be associated with the certificate.</li> </ul> <p>An IP address or DNS name that is associated with the certificate.</p>
Key Length	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.

### 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.

Fields	Description
Select Node	(Required) Choose the Cisco ISE node on which you want to import the system certificate.
Certificate File	(Required) Click <b>Browse</b> to select the certificate file from your local system.
Private Key File	(Required) Click <b>Browse</b> to select the private key file.
Password	(Required) Enter the password to decrypt the private key file.
Friendly Name	Enter a friendly name for the certificate. If you do not specify a name, Cisco ISE automatically creates a name in the format <common name> # <issuer> # <nnnnn> where <nnnnn> is a unique five-digit number.
Allow Wildcard Certificates	Check this check box if you want to import a 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. If you check this check box, Cisco ISE imports this certificate to all the other nodes in the deployment.
Enable Validation of Certificate	Check this check box if you want Cisco ISE to validate the certificate extensions. If you check this check box 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.

Fields	Description
Usage	<p>Choose the service for which this system certificate should be used:</p> <ul style="list-style-type: none"> <li>• Admin—Server certificate used to secure communication with the Admin portal and between ISE nodes in a deployment</li> <li>• EAP Authentication—Server certificate used for authentications that use the EAP protocol for SSL/TLS tunneling</li> <li>• pxGrid—Client and server certificate to secure communication between the pxGrid client and server</li> <li>• Portal—Server certificate used to secure communication with all Cisco ISE web portals</li> </ul>

### 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 50: Certificate Store Page**

Fields	Usage Guidelines
Friendly Name	Displays the name of the certificate.
Status	Enabled or Disabled. If Disabled, ISE will not use the certificate for establishing trust.
Trusted for	Displays the service for which the certificate is used.
Issued To	Common Name (CN) of the certificate subject.
Issued By	Common Name (CN) of the certificate issuer.
Valid From	The “Not Before” certificate attribute.
Expiration Date	The “Not After” certificate attribute.
Expiration Status	<p>Provides information about the status of the certificate expiration. There are five icons and categories of informational message that appear in this column:</p> <ul style="list-style-type: none"> <li>• Green—Expiring in more than 90 days</li> <li>• Blue—Expiring in 90 days or less</li> <li>• Yellow—Expiring in 60 days or less</li> <li>• Orange—Expiring in 30 days or less</li> <li>• Red—Expired</li> </ul>

## Trusted Certificate Edit 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 > Certificate Store > Certificate > Edit**.

**Table 51: Certificate Store Edit Settings**

Fields	Usage Guidelines
Certificate Issuer	
Friendly Name	Enter a friendly name for the certificate.
Status	Choose Enabled or Disabled. If Disabled, ISE will not use the certificate for establishing trust.
Description	Enter an optional description.
Usage	
Trust for authentication within ISE	Check the check box if you want this certificate to verify server certificates (from other ISE nodes or LDAP servers).
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: <ul style="list-style-type: none"> <li>• Authenticate endpoints that connect to ISE using the EAP protocol</li> <li>• Trust a Syslog server</li> </ul>
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.
Certificate Status Validation	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.
Validate Against OCSP Service	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.

Fields	Usage Guidelines
Reject the request if OCSP returns UNKNOWN status	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.
Download CRL	Check the check box for the Cisco ISE to download a CRL.
CRL Distribution URL	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."
Retrieve CRL	The CRL can be downloaded automatically or periodically. Configure the time interval between downloads.
If download failed, wait	Configure the time interval to wait before Cisco ISE tries to download the CRL again.
Bypass CRL Verification if CRL is not Received	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.
Ignore that CRL is not yet valid or expired	<p>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.</p> <p>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.</p>

### 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 52: Trusted Certificate Import Settings**

Fields	Description
Browse	Click <b>Browse</b> to choose the certificate file from the computer that is running the browser.

Fields	Description
Friendly Name	Enter a friendly name for the certificate. If you do not specify a name, Cisco ISE automatically creates a name in the format <common name>#<issuer>#<nnnnn>, where <nnnnn> is a unique five-digit number.
Trust for authentication within ISE	Check the check box if you want this certificate to be used to verify server certificates (from other ISE nodes or LDAP servers).
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: <ul style="list-style-type: none"> <li>• Authenticate endpoints that connect to ISE using the EAP protocol</li> <li>• Trust a Syslog server</li> </ul>
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.
Enable Validation of 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.

### 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 Profile**.

Field	Usage Guidelines
Name	Name of the OCSP Client Profile.
Description	Enter an optional description.
Enable Secondary Server	Check this check box to enable a secondary OCSP server for high availability.
Always Access Primary Server First	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.

Field	Usage Guidelines
Fallback to Primary Server After Interval <i>n</i> Minutes	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.
URL	Enter the URL of the primary and/or secondary OCSP server.
Enable Nonce Extension Support	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.
Validate Response Signature	<p>The OCSP responder signs the response with one of the following certificates:</p> <ul style="list-style-type: none"> <li>• The CA certificate</li> <li>• A certificate different from the CA certificate</li> </ul> <p>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.</p>

Field	Usage Guidelines
Cache Entry Time To Live <i>n</i> Minutes	<p>Enter the time in minutes after which the cache entry expires.</p> <p>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.</p> <p>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.</p> <p>The OCSP cache is used in order to maintain the OCSP responses and for the following reasons:</p> <ul style="list-style-type: none"> <li>• To reduce network traffic and load from the OCSP servers on an already-known certificate</li> <li>• To increase the performance of Cisco ISE by caching already-known certificate statuses</li> </ul>
Clear Cache	<p>Click <b>Clear Cache</b> to clear entries of all the certificate authorities that are connected to the OCSP service.</p> <p>In a deployment, <b>Clear Cache</b> interacts with all the nodes and performs the operation. This mechanism updates every node in the deployment.</p>

## 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.

Fields	Usage Guidelines
Disable Certificate Authority	Click this button to disable the internal CA service.
Host Name	Host name of the Cisco ISE node that is running the CA service.
Personas	Cisco ISE node personas that are enabled on the node running the CA service. For example, Administration, Policy Service, etc.
Role(s)	The role(s) assumed by the Cisco ISE node running the CA service. For example, Standalone or Primary or Secondary.
CA & OCSP Responder Status	Enabled or disabled



Fields	Usage Guidelines
OCSP Responder URL	URL for Cisco ISE node to access the OCSP server.

## 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.



### Note

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.

Fields	Usage Guidelines
Name	(Required) Enter a name for the certificate template. For example, Internal_CA_Template.
Description	(Optional) Enter a description.
Common Name (CN)	(Display only) Common name is autopopulated with the username.
Organizational Unit (OU)	Organizational Unit name. For example, Engineering.
Organization (O)	Organization name. For example, Cisco.
City (L)	(Do not abbreviate) City name. For example, San Jose.
State (ST)	(Do not abbreviate) State name. For example, California.
Country (C)	Country name. You must enter the two-letter ISO country code. For example, US.
Subject Alternative Name (SAN)	(Display only) MAC address of the endpoint.
Key Size	Specify a key size of 1024 or higher.
SCEP RA Profile	Choose the ISE Internal CA or an external SCEP RA profile that you have created.
Valid Period	Enter the number of days after which the certificate expires.

## 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 53: Remote Logging Target Settings**

Fields	Usage Guidelines
Name	Enter the name of the new target.
Target Type	Select the target type. By default it is set to UDP Syslog.
Description	Enter a brief description of the new target.
IP Address	Enter the IP address of the destination machine where you want to store the logs.
Port	Enter the port number of the destination machine.
Facility Code	Choose the syslog facility code to be used for logging. Valid options are Local0 through Local7.
Maximum Length	Enter the maximum length of the remote log target messages. Valid options are from 200 to 1024 bytes.
Buffer Message When Server Down	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.
Buffer Size (MB)	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.
Reconnect Timeout (Sec)	Give in seconds how long will the TCP and secure syslogs be kept before being discarded, when the server is down.
Select CA Certificate	Select a client certificate.

Fields	Usage Guidelines
Ignore Server Certificate Validation	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.

## Logging Category Settings

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 54: Logging Category Settings**

Fields	Usage Guidelines
Name	Displays the name of the logging category.
Log Severity Level	Allows you to choose the severity level for the diagnostic logging categories from the following options: <ul style="list-style-type: none"> <li>• <b>FATAL</b>—Emergency. This option means that Cisco ISE cannot be used and you must take action immediately</li> <li>• <b>ERROR</b>—This option indicates a critical or error condition.</li> <li>• <b>WARN</b>—This option indicates a normal but significant condition. This is the default condition.</li> <li>• <b>INFO</b>—This option indicates an informational message.</li> <li>• <b>DEBUG</b>—This option indicates a diagnostic bug message.</li> </ul>
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.

## 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 55: Repository Settings**

Fields	Usage Guidelines
Repository	Enter the name of the repository. Alphanumeric characters are allowed and the maximum length is 80 characters.
Protocol	Choose one of the available protocols that you want to use.
Server Name	(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.
Path	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.
User Name	(Required for FTP, SFTP, and NFS) Enter the username that has write permission to the specified server. Only alphanumeric characters are allowed.
Password	(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, -, .,  , @, #, \$, %, ^, &, *, (, ), +, and =.

## 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 56: On-Demand Backup Settings**

Fields	Usage Guidelines
Backup Name	Enter the name of your backup file.
Type	Select one of the following: <ul style="list-style-type: none"> <li>• Configuration backup—contains both application-specific and Cisco ADE operating system configuration data.</li> <li>• Operational backup—contains Monitoring and Troubleshooting data.</li> </ul>

Fields	Usage Guidelines
Repository Name	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.
Encryption Key	This key is used to encrypt and decrypt the backup file.

## 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 57: Scheduled Backup Settings**

Fields	Usage Guidelines
Name	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 <b>kron</b> occurrence job.
Description	Enter a description for the backup.
Repository Name	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.
Encryption Key	Enter a key to encrypt and decrypt the backup file.
Schedule Options	Choose the frequency of your scheduled backup and fill in the other options accordingly.

## 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 58: Administrator Password Policy Settings**

Fields	Usage Guidelines
Minimum Length	Specifies the minimum length of the password (in characters). The default is six characters.
Password should not contain the admin name or its characters in reversed order	Check this check box to restrict the use of the administrator username or its characters in reverse order.
Password should not contain 'cisco' or its characters in reversed order	Check this check box to restrict the use of the word "cisco" or its characters in reverse order.
Password should not contain <i>variable</i> or its characters in reversed order	Check this check box to restrict the use of any word that you define or these characters in reverse order.
Password should not contain repeated characters four or more times consecutively	Check this check box to restrict the use of repeated characters four or more times consecutively.
Password must contain at least one character of each of the selected types	Specifies that the administrator password must contain at least one character of the type that you choose from the following choices: <ul style="list-style-type: none"> <li>• Lowercase alphabetic characters</li> <li>• Uppercase alphabetic characters</li> <li>• Numeric characters</li> <li>• Non-alphanumeric characters</li> </ul>
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: <ul style="list-style-type: none"> <li>• 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.)</li> <li>• Reminder (in days) before the administrator account is disabled.</li> </ul>

Fields	Usage Guidelines
Lock or Suspend Account with Incorrect Login Attempts	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.

### Session Timeout and Session Info 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 59: Session Timeout and Session Info Settings**

Fields	Usage Guidelines
Session Timeout	
Session Idle Timeout	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.
Session Info	
Invalidate	Check the check box next to the session ID that you want to terminate and click <b>Invalidate</b> .

## 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 60: Posture General Settings**

Fields	Usage Guidelines
Remediation Timer	Enter a time value in minutes. The default value is 4 minutes. The valid range is 1 to 300 minutes.

Fields	Usage Guidelines
Network Transition Delay	Enter a time value in seconds. The default value is 3 seconds. The valid range is 2 to 30 seconds.
Default Posture Status	Choose Compliant or Noncompliant. The non-agent devices like Linux assumes this status while connecting to the network.
Automatically Close Login Success Screen After	<p>Check the check box to close the login success screen automatically after the specified time.</p> <p>Enter a time value in seconds, in the field next to the check box.</p> <p>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.</p>
Posture Lease	
Perform posture assessment every time a user connects to the network	Select this option to initiate posture assessment every time the user connects to network
Perform posture assessment every <i>n</i> days	Select this option to initiate posture assessment after the specified number of days although the client is already postured Compliant.

### 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 61: Posture Reassessment Configuration Settings**

Fields	Usage Guidelines
Configuration Name	Enter the name of PRA configuration.
Configuration Description	Enter a description for PRA configuration.
Use Reassessment Enforcement?	Check the check box to apply the PRA configurations for the user identity groups.



Fields	Usage Guidelines
Enforcement Type	<p>Choose the action to be enforced:</p> <ul style="list-style-type: none"> <li>• <b>Continue</b> — The user continues to have the privileged access without any user intervention to remediate the client irrespective of the posture requirement.</li> <li>• <b>Logoff</b> — 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.</li> <li>• <b>Remediate</b> — 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.</li> </ul> <p>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.</p> <p>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.</p>
Interval	<p>Enter a time interval in minutes to initiate PRA on the clients after the first successful login.</p> <p>The default value is 240 minutes. Minimum value is 60 minutes and maximum is 1440 minutes.</p>
Grace time	<p>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.</p> <p>The minimum value is 5 minutes and the maximum value is 60 minutes.</p> <p><b>Note</b> The grace time is enabled only when the enforcement type is set to remediate action after the client fails the posture reassessment.</p>
Select User Identity Groups	<p>Choose a unique group or a unique combination of groups for your PRA configuration.</p>
PRA configurations	<p>Displays existing PRA configurations and user identity groups associated to PRA configurations.</p>

## 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 62: Posture AUP Configurations Settings**

Fields	Usage Guidelines
Configuration Name	Enter the name of the AUP configuration that you want to create.
Configuration Description	Enter the description of the AUP configuration that you want to create.
Show AUP to Agent users (for NAC Agent and Web Agent on Windows only)	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.
Use URL for AUP message radio button	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.
Use file for AUP message radio button	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.
AUP URL	Enter the URL to the AUP, which clients must access upon successful authentication and posture assessment.
AUP File	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.

Fields	Usage Guidelines
Select User Identity Groups	<p>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.</p> <p>Note the following while creating an AUP configuration:</p> <ul style="list-style-type: none"> <li>• Posture AUP is not applicable for a guest flow</li> <li>• Each configuration must have a unique user identity group, or a unique combination of user identity groups</li> <li>• No two configurations have any user identity group in common</li> <li>• If you want to create a AUP configuration with a user identity group “Any”, then delete all other AUP configurations first</li> <li>• 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.</li> </ul>
Acceptable use policy configurations—Configurations list	Lists existing AUP configurations and end user identity groups associated with AUP configurations.

## 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 63: Configuring EAP-FAST Settings**

Fields	Usage Guidelines
Authority Identity Info Description	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.
Master Key Generation Period	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.
Revoke all master keys and PACs	Click Revoke to revoke all master keys and PACs.

Fields	Usage Guidelines
Enable PAC-less Session Resume	Check this check box if you want to use EAP-FAST without the PAC files.
PAC-less Session Timeout	Specifies the time in seconds after which the PAC-less session resume times out. The default is 7200 seconds.

### 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 64: Generating PAC for EAP-FAST Settings**

Fields	Usage Guidelines
Tunnel PAC	Click this radio button to generate a tunnel PAC.
Machine PAC	Click this radio button to generate a machine PAC.
Trustsec PAC	Click this radio button to generate a Trustsec PAC.
Identity	(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.
PAC Time to Live	(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.
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.
Expiration Data	(For Trustsec PAC only) The expiration date is calculated based on the PAC Time to Live.

## 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 65: EAP-TLS Settings**

Fields	Usage Guidelines
Enable EAP-TLS Session Resume	Check this check box to support an abbreviated reauthentication of a user who has passed full EAP-TLS 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.
EAP-TLS Session Timeout	Specifies the time in seconds after which the EAP-TLS session times out. The default value is 7200 seconds.

## 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 66: PEAP Settings**

Fields	Usage Guidelines
Enable PEAP Session Resume	Check this check box for the Cisco ISE to cache the TLS session that is created during phase one of PEAP authentication, provided the user successfully authenticates in phase two of PEAP. If a user needs to reconnect and the original PEAP session has not timed out, the Cisco ISE uses the cached TLS session, resulting in faster PEAP performance and a reduced AAA server load. You must specify a PEAP session timeout value for the PEAP session resume features to work.
PEAP Session Timeout	Specifies the time in seconds after which the PEAP session times out. The default value is 7200 seconds.
Enable Fast Reconnect	Check this check box to allow a PEAP session to resume in the Cisco ISE without checking user credentials when the session resume feature is enabled.

## RADIUS Settings

The following table describes the fields on the RADIUS Settings page, which you can use to detect the clients that fail to authenticate and to suppress the repeated reporting of successful authentications. The navigation path for this page is: **Administration > System > Settings > Protocols > RADIUS**.

When you enable anomalous client suppression and an endpoint authentication fails twice within the configured detection interval, Cisco ISE marks the supplicant as misconfigured and suppresses additional failed authentications with the same failure reason. You can find more details about the suppression by clicking the Misconfigured Supplicant Counter link on the Live Authentications page. A successful authentication from a suppressed endpoint clears the suppression, and results in a decrease in the Misconfigured Supplicant Counter value on the Live Authentications page. Also, if there is no authentication activity from the suppressed endpoint for a period of six hours, the suppression is cleared automatically.

Cisco ISE allows you to enable strong suppression by enabling the Reject Requests After Detection option. If you check the Reject Requests After Detection check box, and an endpoint authentication fails five times with the same failure reason, Cisco ISE activates strong suppression. All subsequent authentications, whether successful or not, are suppressed, and authentication does not occur. This “strong” suppression is cleared after the configured Request Rejection Interval elapses or after six hours of authentication inactivity from the endpoint.

**Table 67: RADIUS Settings**

Fields	Usage Guidelines
Suppress Anomalous Clients	Check this check box to detect the clients for which the authentications fail repeatedly. A summary of the failures will be reported every Reporting Interval.
Detection Interval	Enter the time interval in minutes for the clients to be detected.
Reporting Interval	Enter the time interval in minutes for the failed authentications to be reported.
Reject Requests After Detection	Check this check box to reject the requests from a client that is identified as anomalous or misconfigured. The requests from anomalous clients will be rejected during the Request Rejection Interval.
Request Rejection Interval	Enter the time interval in minutes for which the requests are to be rejected. This option is available only when you have checked Reject Requests After Detection check box.
Suppress Repeated Successful Authentications	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.
Accounting Suppression Interval	Enter the time interval in seconds for which the reporting of accounting requests to be suppressed.
Long Processing Step Threshold Interval	Enter the time interval in milliseconds. The steps are displayed in authentication details reports. If execution of a single step exceeds the specified threshold, then it will be highlighted in the authentication details report.

## TrustSec Settings

For Cisco ISE to function as a TrustSec server and provide TrustSec services, you must define the global TrustSec settings. The following table describes the fields on the TrustSec Settings page. The navigation path for this page is: **Administration > System > Settings > TrustSec Settings**.

**Table 68: Configuring TrustSec Settings**

Fields	Usage Guidelines
Tunnel PAC Time to Live	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: <ul style="list-style-type: none"> <li>• 1 to 157680000 seconds</li> <li>• 1 to 2628000 minutes</li> <li>• 1 to 43800 hours</li> <li>• 1 to 1825 days</li> <li>• 1 to 260 weeks</li> </ul>
Proactive PAC Update Will Occur After	Cisco ISE proactively provides a new PAC to the 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 happens before the PAC expiration. This mechanism allows the client to be always updated with a valid PAC. The default value is 10%.

## SMS Gateway Settings

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 email server.

**Table 69: SMS Gateway Settings for SMS Email Gateway**

Field	Usage Guidelines
SMS Gateway Provider Domain	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.
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 <b>Default Email Address</b> global setting in <b>Guest Access &gt; Settings</b> .

Field	Usage Guidelines
SMTP API destination address	<p>(Optional)</p> <p>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.</p> <p>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.</p>
SMTP API body template	<p>(Optional)</p> <p>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.</p> <p>The supported dynamic substitutions are \$mobilenumber\$ and \$message\$.</p>

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 70: SMS Gateway Settings for SMS HTTP API**

Field	Usage Guidelines
URL	<p>Enter the URL for the API.</p> <p>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\$.</p> <p>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 <b>Administration &gt; System &gt; Certificates &gt; Trusted Certificates</b>.</p>
Data (Url encoded portion)	<p>Enter the Data (Url encoded portion) for the GET or POST request.</p> <p>This field is URL encoded. If using the default GET method, the data is appended to the URL specified above.</p>



Field	Usage Guidelines
Use HTTP POST method for data portion	If using the POST method, check this option. The data specified above is used as the content of the POST request.
HTTP POST data content type	If using the POST method, specify the content type such as "plain/text" or "application/xml".
HTTPS Username HTTPS Password HTTPS Host name HTTPS Port number	Enter this information.

## 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: Administration > Identity Management > Identities > Endpoints.

**Table 71: Endpoint Settings**

Fields	Usage Guidelines
MAC Address	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
Static Assignment	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.

Fields	Usage Guidelines
Policy Assignment	<p>(Disabled by default unless the Static Assignment is checked) Choose a matching endpoint policy from the Policy Assignment drop-down list.</p> <p>You can do one of the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
Static Group Assignment	<p>(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.</p> <p>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.</p> <p>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.</p>
Identity Group Assignment	<p>Choose an endpoint identity group to which you want to assign the endpoint.</p> <p>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.</p> <p>Cisco ISE includes the following system created endpoint identity groups:</p> <ul style="list-style-type: none"> <li>• Blacklist</li> <li>• GuestEndpoints</li> <li>• Profiled <ul style="list-style-type: none"> <li>◦ Cisco IP-Phone</li> <li>◦ Workstation</li> </ul> </li> <li>• RegisteredDevices</li> <li>• Unknown</li> </ul>

## 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: **Administration > Identity Management > Identities > Endpoints**.

**Table 72: Endpoint Import from LDAP Settings**

Fields	Usage Guidelines
Connection Settings	
Host	Enter the hostname, or the IP address of the LDAP server.
Port	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.  <b>Note</b> Cisco ISE supports any configured port number. The configured value should match the LDAP server connection details.
Enable Secure Connection	Check the Enable Secure Connection check box to import from an LDAP server over SSL.
Root CA Certificate Name	Click the drop-down arrow to view the trusted CA certificates.  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.
Anonymous Bind	Check the Anonymous Bind check box to enable the anonymous bind.  You must enable either the Anonymous Bind check box, or enter the LDAP administrator credentials from the slapd.conf configuration file.
Admin DN	Enter the distinguished name (DN) configured for the LDAP administrator in the slapd.conf configuration file.  Admin DN format example: cn=Admin, dc=cisco.com, dc=com
Password	Enter the password configured for the LDAP administrator in the slapd.conf configuration file.
Base DN	Enter the distinguished name of the parent entry.  Base DN format example: dc=cisco.com, dc=com.
Query Settings	
MAC Address objectClass	Enter the query filter, which is used for importing the MAC address. For example, ieee802Device.
MAC Address Attribute Name	Enter the returned attribute name for import. For example, macAddress.

Fields	Usage Guidelines
Profile Attribute Name	<p>Enter the name of the LDAP attribute. This attribute holds the policy name for each endpoint entry that is defined in the LDAP server.</p> <p>When you configure the Profile Attribute Name field, consider the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
Time Out [seconds]	Enter the time in seconds between 1 and 60 seconds.

## 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 73: Endpoint Identity Group Settings**

Fields	Usage Guidelines
Name	Enter the name of the endpoint identity group that you want to create.
Description	Enter a description for the endpoint identity group that you want to create.

Fields	Usage Guidelines
Parent Group	<p>Choose an endpoint identity group from the Parent Group drop-down list to which you want to associate the newly created endpoint identity group.</p> <p>Cisco ISE includes the following five endpoint identity groups:</p> <ul style="list-style-type: none"> <li>• Blacklist</li> <li>• GuestEndpoints</li> <li>• Profiled</li> <li>• RegisteredDevices</li> <li>• Unknown</li> </ul> <p>In addition, it creates two more identity groups, Cisco-IP-Phone and Workstation, which are associated to the Profiled (parent) identity group.</p>

## 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 74: LDAP General Settings**

Fields	Usage Guidelines
Name	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.
Description	Enter a description for the LDAP instance. This value is of type string, and has a maximum length of 1024 characters.

Fields	Usage Guidelines
Schema	<p>You can choose any one of the following built-in schema types or create a custom schema:</p> <ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Sun Directory Server</li> <li>• Novell eDirectory</li> </ul> <p>You can click the arrow next to Schema to view the schema details.</p> <p>If you edit the attributes of the predefined schema, Cisco ISE automatically creates a Custom schema.</p>
<b>Note</b> The following fields can be edited only when you choose the Custom schema.	
Subject Objectclass	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.
Subject Name Attribute	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.
Certificate Attribute	Enter the attribute that contains the certificate definitions. For certificate-based authentication, these definitions are used to validate certificates that are presented by clients.
Group Objectclass	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.
Group Map Attribute	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.
Subject Objects Contain Reference To Groups	Click this radio button if the subject objects contain an attribute that specifies the group to which they belong.
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.

### LDAP Connection Settings

The following table describes the fields in the Connection Settings tab.

**Table 75: 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 (-).
Port	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.
Access	<p>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.</p> <p>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.
Server Timeout	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.

Fields	Usage Guidelines
Max. Admin Connections	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.
Test Bind to Server	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.
Failover	
Always Access Primary Server First	Click this option if you want Cisco ISE to always access the primary LDAP server first for authentications and authorizations.
Failback to Primary Server After	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.

### LDAP Directory Organization Settings

The following table describes the fields in the Directory Organization tab.

**Table 76: LDAP Directory Organization Settings**

Fields	Usage Guidelines
Subject Search Base	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.



Fields	Usage Guidelines
Group Search Base	<p>Enter the DN for the subtree that contains all groups. For example:  ou=organizational unit, ou=next organizational unit, o=corporation.com</p> <p>If the tree containing groups is the base DN, type:  o=corporation.com</p> <p>or  dc=corporation,dc=com</p> <p>as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.</p>
Search for MAC Address in Format	<p>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.</p> <p>Use the drop-down list to enable searching for MAC addresses in a specific format, where <i>&lt;format&gt;</i> can be any one of the following:</p> <ul style="list-style-type: none"> <li>• xxxx.xxxx.xxxx</li> <li>• xxxxxxxxxxxx</li> <li>• xx-xx-xx-xx-xx-xx</li> <li>• xx:xx:xx:xx:xx:xx</li> </ul> <p>The format you choose must match the format of the MAC address sourced in the LDAP server.</p>
Strip Start of Subject Name Up To the Last Occurrence of the Separator	<p>Enter the appropriate text to remove domain prefixes from usernames.</p> <p>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 <i>&lt;start_string&gt;</i> 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.</p> <p><b>Note</b> The <i>&lt;start_string&gt;</i> cannot contain the following special characters: the pound sign (#), the question mark (?), the quotation mark ("), the asterisk (*), the right angle bracket (&gt;), and the left angle bracket (&lt;). Cisco ISE does not allow these characters in usernames.</p>

Fields	Usage Guidelines
Strip End of Subject Name from the First Occurrence of the Separator	<p>Enter the appropriate text to remove domain suffixes from usernames.</p> <p>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 <i>user1@domain</i>, then Cisco ISE submits <i>user1</i> to the LDAP server.</p> <p><b>Note</b> The <i>&lt;end_string&gt;</i> box cannot contain the following special characters: the pound sign (#), the question mark (?), the quotation mark ("), the asterisk (*), the right angle bracket (&gt;), and the left angle bracket (&lt;). Cisco ISE does not allow these characters in usernames.</p>

### LDAP Group Settings

**Table 77: LDAP Group Settings**

Fields	Usage Guidelines
Add	<p>Choose <b>Add &gt; Add Group</b> to add a new group or choose <b>Add &gt; Select Groups From Directory</b> to select the groups from the LDAP directory.</p> <p>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 <b>Retrieve Groups</b>. 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.</p>

### LDAP Attribute Settings

**Table 78: LDAP Attribute Settings**

Fields	Usage Guidelines
Add	<p>Choose <b>Add &gt; Add Attribute</b> to add a new attribute or choose <b>Add &gt; Select Attributes From Directory</b> to select attributes from the LDAP server.</p> <p>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 <b>Retrieve Attributes</b> to retrieve the user's attributes. Check the check boxes next to the attributes that you want to select, and then click OK.</p>

## 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 79: RADIUS Token Identity Source Settings**

Fields	Usage Guidelines
Name	Enter a name for the RADIUS token server. The maximum number of characters allowed is 64.
Description	Enter a description for the RADIUS token server. The maximum number of characters is 1024.
SafeWord Server	Check this check box if your RADIUS identity source is a SafeWord server.
Enable Secondary Server	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.
Always Access Primary Server First	Click this radio button if you want Cisco ISE to always access the primary server first.
Fallback to Primary Server after	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.
<b>Primary Server</b>	
Host IP	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 (.).
Shared Secret	Enter the shared secret that is configured on the primary RADIUS token server for this connection.
Authentication Port	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.
Server Timeout	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.
Connection Attempts	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.

Fields	Usage Guidelines
<b>Secondary Server</b>	
Host IP	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 (.).
Shared Secret	Enter the shared secret configured on the secondary RADIUS token server for this connection.
Authentication Port	Enter the port number on which the secondary RADIUS token server is listening. Valid values are from 1 to 65,535. The default is 1812.
Server Timeout	Specify the time in seconds that Cisco ISE should wait for a response from the secondary RADIUS token server before it determines that the secondary server is down. Valid values are 1 to 300. The default is 5.
Connection Attempts	Specify the number of attempts that Cisco ISE should make to reconnect to the secondary server before dropping the request. Valid values are 1 to 9. The default is 3.

### 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 80: RSA Prompt Settings**

Fields	Usage Guidelines
Enter Passcode Prompt	Enter a text string to obtain the passcode.
Enter Next Token Code	Enter a text string to request the next token.
Choose PIN Type	Enter a text string to request the PIN type.
Accept System PIN	Enter a text string to accept the system-generated PIN.
Enter Alphanumeric PIN	Enter a text string to request an alphanumeric PIN.
Enter Numeric PIN	Enter a text string to request a numeric PIN.

Fields	Usage Guidelines
Re-enter PIN	Enter a text string to request the user to re-enter the PIN.

### RSA Message Settings

The following table describes the fields in the RSA Messages tab.

**Table 81: RSA Messages Settings**

Fields	Usage Guidelines
Display System PIN Message	Enter a text string to label the system PIN message.
Display System PIN Reminder	Enter a text string to inform the user to remember the new PIN.
Must Enter Numeric Error	Enter a message that instructs users to enter only numbers for the PIN.
Must Enter Alpha Error	Enter a message that instructs users to enter only alphanumeric characters for PINs.
PIN Accepted Message	Enter a message that the users see when their PIN is accepted by the system.
PIN Rejected Message	Enter a message that the users see when the system rejects their PIN.
User Pins Differ Error	Enter a message that the users see when they enter an incorrect PIN.
System PIN Accepted Message	Enter a message that the users see when the system accepts their PIN.
Bad Password Length Error	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.

## Identity Management Settings

### User Password Policy Settings

The following table describes the fields on the User Password Policy page, which you can use to define a criteria for user passwords. The navigation path for this page is: **Administration > Identity Management > Settings > Password Policy**.

**Table 82: User Password Policy Settings**

Option	Description
Minimum Length	Sets the minimum length of password (in characters)
Username	Restricts the use of the username or its characters in reversed order
Cisco	Restricts the use of "cisco" or its characters in reversed order
Special characters	Restricts the use of special characters that you define in reverse order
Repeated characters	Restricts the use of characters repeated four or more times consecutively
Required characters	<p>Requires that the password include at least one of each of the following types:</p> <ul style="list-style-type: none"> <li>• Lowercase alphabetic characters</li> <li>• Uppercase alphabetic characters</li> <li>• Numeric characters</li> <li>• Non-alphanumeric characters</li> </ul>
Password History	<p>Enter the number of previous versions from which the password must be different to prevent the repeated use of the same password</p> <p>You can also enter the number of characters that must be different from the previous password</p> <p>Enter the number of days before which you cannot reuse a password</p>
Password Lifetime	<p>Sets the following options to force users to change passwords after a specified time period:</p> <ul style="list-style-type: none"> <li>• Time (in days) before the user account is disabled if the password is not changed</li> <li>• Reminder (in days) before the user account is disabled</li> </ul>
Lock or Suspend Account with Incorrect Login Attempts	<p>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.</p> <p>An e-mail is sent to the administrator whose account gets locked out. You can enter a custom e-mail remediation message.</p>

# Network Resources

## Network Devices

These pages enable you to add and manage network devices.

### Network Device Definition Settings

The following table describes the fields on 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 83: Network Device Settings**

Fields	Description
Name	<p>Enter the name for the network device.</p> <p>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.</p> <p><b>Note</b> You cannot edit the name of a device once configured.</p>
Description	<p>Enter the description for the device.</p>
IP Address/Mask	<p>Enter a single IP address and a subnet mask.</p> <p>The following are the guidelines that must be followed while defining the IP addresses and subnet masks:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• You cannot define two devices with the same specific IP addresses.</li> <li>• You cannot define two devices with the same IP range. The IP ranges must not overlap either partially or completely.</li> </ul>
Model Name	<p>Click the drop-down list to choose the device model, for example.</p> <p>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.</p>

Fields	Description
Software Version	<p>Click the drop-down list d to choose the version of the software running on the network device.</p> <p>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.</p>
Network Device Group	<p>Click the Location and Device Type drop-down lists to choose a location and device type that can be associated with the network device.</p> <p>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.</p>

### RADIUS Authentication Settings

The following table describes the fields in the RADIUS Authentication Settings section.

**Table 84: RADIUS Authentication Settings**

Fields	Usage Guidelines
Protocol	Displays RADIUS as the selected protocol.
Shared Secret	<p>Enter a shared secret, which can be up to 127 characters in length.</p> <p>The shared secret is the key that you have configured on the network device using the <b>radius-host</b> command with the <b>pac</b> option.</p>
Enable KeyWrap	<p>Check this check box only when supported on the network device, which increases RADIUS security via an AES KeyWrap algorithm.</p> <p><b>Note</b> When you run Cisco ISE in FIPS mode, you must enable KeyWrap on the network device.</p>
Key Encryption Key	(Only appears when you enable KeyWrap) Enter an encryption key that is used for session encryption (secrecy).
Message Authenticator Code Key	(Only appears when you enable KeyWrap) Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages.



Fields	Usage Guidelines
Key Input Format	<p>Choose one of the following formats:</p> <ul style="list-style-type: none"> <li>• <b>ASCII</b>—The Key Encryption Key must be 16 characters (bytes) long, and the Message Authenticator Code Key must be 20 characters (bytes) long.</li> <li>• <b>Hexadecimal</b>—The Key Encryption Key must be 32 bytes long, and the Message Authenticator Code Key must be 40 bytes long.</li> </ul> <p>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, and shorter values are not permitted.)</p>

### SNMP Settings

The following table describes the fields in the SNMP Settings section.

**Table 85: SNMP Settings**

Fields	Usage Guidelines
SNMP Version	<p>Choose an SNMP version from the Version drop-down list to be used for requests.</p> <p>Version includes the following:</p> <ul style="list-style-type: none"> <li>• 1—SNMPv1 does not support informs.</li> <li>• 2c</li> <li>• 3—SNMPv3 is the most secure model because it allows packet encryption when you choose the Priv security level.</li> </ul> <p><b>Note</b> 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.</p>
SNMP RO Community	(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.
SNMP Username	(Only for SNMP Version 3) Enter SNMP username.

Fields	Usage Guidelines
Security Level	<p>(Only for SNMP Version 3) Choose the security level from the following:</p> <ul style="list-style-type: none"> <li>• Auth—Enables Message Digest 5 or Secure Hash Algorithm (SHA) packet authentication</li> <li>• No Auth—No authentication and no privacy security level</li> <li>• Priv—Enables Data Encryption Standard (DES) packet encryption</li> </ul>
Auth Protocol	<p>(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.</p> <p>Authentication Protocol includes one of the following for security levels of Auth and Priv:</p> <ul style="list-style-type: none"> <li>• MD5</li> <li>• SHA</li> </ul>
Auth Password	<p>(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.</p> <p>Click <b>Show</b> to display the Auth Password that is already configured for the device.</p>
Privacy Protocol	<p>(Only for SNMP Version 3 when the security level Priv is selected) Choose the privacy protocol that you want the network device to use.</p> <p>Privacy Protocols are one of the following:</p> <ul style="list-style-type: none"> <li>• DES</li> <li>• AES128</li> <li>• AES192</li> <li>• AES256</li> <li>• 3DES</li> </ul>
Privacy Password	<p>(Only for SNMP Version 3 when the security level Priv is selected) Enter the privacy key.</p> <p>Click <b>Show</b> to display the Privacy Password that is already configured for the device.</p>
Polling Interval	Enter the polling interval in seconds. The default is 3600 seconds.
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

Fields	Usage Guidelines
Originating Policy Service Node	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.

### Advanced Trustsec Settings

The following table describes the fields in the Advanced Trustsec Settings section.

**Table 86: Advanced Trustsec Settings**

Fields	Usage Guidelines
Trustsec Device Notification and Updates Settings	
Use Device ID for Trustsec Identification	Check this check box if you want the Device Name to be listed as the device identifier in the Device ID field.  If you check this check box, then the Device Name appears in the Device Id field. You can also change this Device Id to a descriptive name of your choice.
Device Id	(Only when the Use Device ID for Trustsec Identification check box is not checked). You can use the Device Name as the logical identifier when populated in this field.
Password	Enter the password to authenticate the Trustsec device (the same password that you have configured on the Trustsec device command-line interface [CLI]).  Click <b>Show</b> to display the password that is used to authenticate the Trustsec device.
Download Environment Data Every	Specify the expiry time that allows you to configure the time interval in seconds, minutes, hours, weeks, or days between to download the Trustsec device environment information from Cisco ISE.  For example, if you enter 60 in seconds, the device would download its environment data from Cisco ISE every minute. The default value is 86,400 seconds or one day. The valid range is from 1 to 24850.
Download Peer Authorization Policy Every	Specify the expiry time that allows you to configure the time interval in seconds, minutes, hours, weeks, or days between to download the peer authorization policy from Cisco ISE.  For example, if you enter 60 in seconds, the device would download its peer authorization policy from Cisco ISE every minute. The default value is 86,400 seconds or one day. The valid range is from 1 to 24850.

Fields	Usage Guidelines
Reauthentication Every	<p>Specify the 802.1X reauthentication period that allows you to configure the time interval in seconds, minutes, hours, weeks or days between for reauthentication.</p> <p>In a network that is configured with the Trustsec solution, after initial authentication, the Trustsec device re authenticates itself against Cisco ISE.</p> <p>For example, if you enter 1000 seconds, the device would authenticate itself against Cisco ISE every 1000 seconds. The default value is 86,400 seconds or one day. The valid range is from 1 to 24850.</p>
Download SGACL Lists Every	<p>Specify the expiry time for SGACL lists that allow you to configure the time interval in seconds, minutes, hours, weeks or days between to download SGACLs from Cisco ISE.</p> <p>For example, if you enter 3600 seconds, the network device obtains the SGACL lists from Cisco ISE every 3600 seconds. The default value is 86,400 seconds or one day. The valid range is from 1 to 24850.</p>
Other Trustsec Devices to Trust This Device (Trustsec Trusted)	<p>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 packets that arrive from this device will be colored or tagged accordingly.</p>
Notify this device about Trustsec configuration changes	<p>Check this check box if you want Cisco ISE to send Trustsec CoA notifications to this Trustsec device.</p>
Device Configuration Deployment Settings	
Include this device when deploying Security Group Tag Mapping Updates	<p>Check this check box if you want this Trustsec device to obtain the IP-SGT mappings using device interface credentials.</p>
Exec Mode Username	<p>Enter the username that has privileges to edit the device configuration in the Exec mode.</p>
Exec Mode Password	<p>Enter the password of the user having privileges to edit the device configuration in the Exec mode.</p>
Enable Mode Password	<p>Enter the password to enable Exec mode password for the device that would allow you to edit its configuration.</p> <p>Click <b>Show</b> to display the Exec mode password that is already configured for this device.</p>
Out Of Band (OOB) Trustsec PAC Display	
Issue Date	<p>Displays the issuing date of the last Trustsec PAC that has been generated by Cisco ISE for this Trustsec device.</p>

Fields	Usage Guidelines
Expiration Date	Displays the expiration date of the last Trustsec PAC that has been generated by Cisco ISE for this 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 this device.
Generate PAC	Click Generate PAC to create Trustsec Protected Access Credentials (PAC). By default, Out Of Band Trustsec Protected Access Credentials (PAC) information is empty, but appears disabled when populated. Trustsec PAC information can be automatically populated when you generate Trustsec PAC for any Trustsec enabled device.

### Default Network Device Definition Settings

The following table describes the fields on the Default Network device page, which allows you to configure a default network device that Cisco ISE can use for RADIUS authentications. The navigation path for this page is: **Administration > Network Resources > Network Devices > Default Device**.

**Table 87: Default Network Device Definition Settings**

Fields	Usage Guidelines
Default Network Device Status	Choose <b>Enable</b> from the Default Network Device Status drop-down list to enable the default network device definition.
Protocol	Displays RADIUS as the selected protocol.
Shared Secret	Enter the shared secret that can be up to 128 characters in length. The shared secret is the key that you have configured on the network device using the <b>radius-host</b> command with the <b>pac</b> option.
Enable KeyWrap	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.
Key Encryption Key	Enter an encryption key that is used for session encryption (secrecy) when you enable KeyWrap.
Message Authenticator Code Key	Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages when you enable KeyWrap.

Fields	Usage Guidelines
Key Input Format	<p>Choose one of the following formats:</p> <ul style="list-style-type: none"> <li>• <b>ASCII</b>—The Key Encryption Key must be 16 characters (bytes) long, and the Message Authenticator Code Key must be 20 characters (bytes) long.</li> <li>• <b>Hexadecimal</b>—The Key Encryption Key must be 32 bytes long, and the Message Authenticator Code Key must be 40 bytes long.</li> </ul> <p>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, and shorter values are not permitted.)</p>

### 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 88: Network Devices Import Settings**

Fields	Usage Guidelines
Generate a Template	<p>Click this link to create a comma-separated value (.csv) template file.</p> <p>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.</p>
File	<p>Click <b>Browse</b> to the location of the comma-separated value file that you might have created or previously exported from any Cisco ISE deployment.</p> <p>You can import network devices in another Cisco ISE deployment with new and updated network devices information using import.</p>
Overwrite Existing Data with New Data	<p>Check this check box if you want Cisco ISE to replace existing network devices with the devices in your import file.</p> <p>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.</p>
Stop Import on First Error	<p>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.</p> <p>If this check box is not checked and an error is encountered, the error is reported, and Cisco ISE continues to import devices.</p>

## 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**.

**Table 89: Network Device Group Settings**

Fields	Usage Guidelines
Name	<p>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.</p> <p>The full name of the Network Device Group that can have a maximum of 100 characters. 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 should not exceed 100 characters. If the full name of the NDG exceeds 100 characters, the NDG creation fails.</p>
Description	Enter the description for the root or the child Network Device Group.
Type	<p>Enter the type for the root Network Device Group.</p> <p>For all subsequent child network device groups under the root NDG, the type is inherited from the parent NDG and therefore all the child NDGs under a root NDG will be of the same type.</p> <p>If this NDG is a root NDG, then the type will be available as an attribute in the device dictionary. You can define conditions based on this attribute. The name of the NDG is one of the values that this attribute can take.</p>

### 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 90: Network Device Groups Import Settings**

Fields	Usage Guidelines
Generate a Template	<p>Click this link to create a comma-separated value (.csv) template file.</p> <p>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.</p>

Fields	Usage Guidelines
File	Click <b>Browse</b> 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 device groups in another Cisco ISE deployment with new and updated network device groups information using import.
Overwrite Existing Data with New Data	Check this check box if you want Cisco ISE to replace existing network device groups with the device groups in your import file.  If you do not check this check box, new network device group that are available in the import file are added to the network device group repository. Duplicate entries are ignored.
Stop Import on First Error	Check this check box if you want Cisco ISE to discontinue import when it encounters an error during import, but Cisco ISE imports network device groups 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 device groups.

## 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 91: External RADIUS Server Settings**

Fields	Usage Guidelines
Name	Enter the name of the external RADIUS server.
Description	Enter a description of the external RADIUS server.
Host IP	Enter the IP address of the external RADIUS server.
Shared Secret	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.
Enable KeyWrap	Enable this option to increase the RADIUS protocol security via an AES KeyWrap algorithm, to help enable FIPS 140-2 compliance in Cisco ISE.
Key Encryption Key	(Only if you check the Enable Key Wrap check box) Enter a key to be used for session encryption (secrecy).



Fields	Usage Guidelines
Message Authenticator Code Key	(Only if you check the Enable Key Wrap check box) Enter a key to be used for keyed HMAC calculation over RADIUS messages.
Key Input Format	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.) <ul style="list-style-type: none"> <li>• ASCII—The Key Encryption Key must be 16 characters (bytes) long, and the Message Authenticator Code Key must be 20 characters (bytes) long.</li> <li>• Hexadecimal—The Key Encryption Key must be 32 bytes long, and the Message Authenticator Code Key must be 40 bytes long.</li> </ul>
Authentication Port	Enter the RADIUS authentication port number. The valid range is from 1 to 65535. The default is 1812.
Accounting Port	Enter the RADIUS accounting port number. The valid range is from 1 to 65535. The default is 1813.
Server Timeout	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.
Connection Attempts	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.

## 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 92: RADIUS Server Sequences**

Fields	Usage Guidelines
Name	Enter the name of the RADIUS server sequence.
Description	Enter an optional description.
Host IP	Enter the IP address of the external RADIUS server.
User Selected Service Type	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.
Remote Accounting	Check this check box to enable accounting in the remote policy server.

Fields	Usage Guidelines
Local Accounting	Check this check box to enable accounting in Cisco ISE.
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	<p>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.</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul>
Modify Attributes in the Request to the External RADIUS Server	<p>Check this check box to allow Cisco ISE to manipulate attributes that come from or go to the authenticated RADIUS server.</p> <p>The attribute manipulation operations include these:</p> <ul style="list-style-type: none"> <li>• <b>Add</b>—Add additional attributes to the overall RADIUS request/response.</li> <li>• <b>Update</b>—Change the attribute value (fixed or static) or substitute an attribute by another attribute value (dynamic).</li> <li>• <b>Remove</b>—Remove an attribute or an attribute-value pair.</li> <li>• <b>RemoveAny</b>—Remove any occurrences of the attribute.</li> </ul>
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.

## 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 93: NAC Manager Settings**

Fields	Usage Guidelines
Name	Enter the name of the Cisco Access Manager (CAM).
Status	Click the Status check box to enable REST API communication from the Cisco ISE profiler that authenticates connectivity to the CAM.
Description	Enter the description of the CAM.
IP Address	<p>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.</p> <p>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.</p> <p><b>Note</b> 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.</p>
Username	Enter the username of the CAM administrator that allows you to log on to the user interface of the CAM.
Password	Enter the password of the CAM administrator that allows you to log on to the user interface of the CAM.

## Device Portal Management

### Configure Device Portal Settings

#### Global Settings for Device Portals

Choose **Administration > Device Portal Management > Settings**.

You can configure the following general settings for the BYOD and My Devices portals:

- The maximum number of personal devices that an employee can register at any time using either portal.
- An IP address or URL that will reconnect an employee device to the BYOD registration process if a problem is encountered during the process.

Once you configure these general settings, they apply to all BYOD and My Devices portals that you set up for your company.

### Portal Identification Settings for Device Portals

The navigation path for these settings is **Administration > Device Portal Management > Blacklist Portal, Client Provisioning Portals, BYOD Portals, MDM Portals, or My Device Portals > Create, Edit or Duplicate > Portals Settings and Customization**.

Use these settings to identify the portal and select the language files to be used for all the portal pages.

Field	Usage Guidelines
Portal Name	<p>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.</p> <p>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.</p>
Description	Optional.
Portal test URL	<p>A system-generated URL displays as a link after you click <b>Save</b>. Use it to test the portal.</p> <p>Click the link to open a new browser tab that displays the URL for this portal that is being served by a Policy Services Node (PSN) with Policy Services turned on. If Policy Services are not turned on, the PSN will not serve web pages for any portals other than the Admin portal.</p> <p><b>Note</b> 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.</p>

Field	Usage Guidelines
Language File	<p>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.</p> <p>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.</p> <p>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.</p>

### 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).

- **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 ISE and were using Port values outside this range, they are honored until you make any change to this page. If you do change this page, you must 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.

- **Allowed interfaces**—Select the PSN interfaces where this portal can run. 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.
  - The Ethernet interfaces must use IP addresses on different subnets.
  - The interfaces you enable here must be available on all the PSNs that are running portals, 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. If the interface IP is not the same as the domain, then configure **ip host x.x.x.x yyy.domain.com** in the ISE CLI to map your interface IP to FQDN in the certificate.
- **Certificate group tag**—Select the group tag of the certificate group to use for the portal’s HTTPS traffic.
- **Display Language**—Specify which language is used in the portal: the user’s browser locale setting, with a fallback to another language if a browser locale is not available. Or force the portal to always use one language.

### Portal Settings for BYOD Device Registration 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 change this page. If you do change 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 will display.
- **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 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 is used to match Certificate Subject Name / Alternate Subject Name.
- **Certificate group tag**—Select the group tag of the certificate group 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 additional 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 additional endpoint identity groups if you choose to not use the default.
- **Use Browser Locale**—Specify that the user’s browser locale setting is used for the display language of the portal. This assumes that the language file has a language that is mapped to the browser locale. If not, the Fallback Language will be used for the text displayed in the portal.
- **Fallback Language**—Choose the language to use if a language file is not available for the browser locale.

- Always Use—Choose the display language to use for the portal. This setting overrides the User browser locale option.

### 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.

Field	Usage Guidelines
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 their account is fully enabled. The <b>Login</b> 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 <b>Include an AUP on page</b> is enabled.  Ensure that the user has read the AUP completely. The <b>Accept</b> button activates only after the user has scrolled to the end of the AUP.
Display Device ID field during registration	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 .
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 performs the provisioning. Therefore, these devices are not redirected to the originating URL. However, iOS (dot1X) and unsupported devices (that are allowed network access) will be redirected to this URL.

Field	Usage Guidelines
Success page	Display a page indicating that the device registration was successful.
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.

### Portal Settings for Client Provisioning Portals

The navigation path for these settings is **Administration > Device Portal Management > Client Provisioning 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 change this page. If you do change 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 will display.
- **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 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 is used to match Certificate Subject Name / Alternate Subject Name.
- **Certificate group tag**—Select the group tag of the certificate group to use for the portal's HTTPS traffic.
- **Display Language**—Specify which language is used in the portal: the user's browser locale setting, with a fallback to another language if a browser locale is not available. Or force the portal to always use one language.



## 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.

Field	Usage Guidelines
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 their account is fully enabled. The <b>Login</b> 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 <b>Include an AUP on page</b> is enabled.  Ensure that the user has read the AUP completely. The <b>Accept</b> button activates only after the user has scrolled to the end of the AUP.

## 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 change this page. If you do change 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 will display.
- **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 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 is used to match Certificate Subject Name / Alternate Subject Name.
- **Certificate group tag**—Select the group tag of the certificate group to use for the portal’s HTTPS traffic.
- **Fully Qualified Domain Name (FQDN)**—Enter at least one unique FQDN or hostname for your Sponsor or MyDevices portal. For example, you can enter `entersponsorportal.yourcompany.com,sponsor`, so that when the user enters either of those into a browser, they reach the sponsor portal. Separate names with commas, but do not include spaces between entries. Cisco ISE includes a default sponsor Identity Source Sequence for sponsor portals, `Sponsor_Portal_Sequence`.
  - 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.

If you choose to update the default FQDN, also do the following:

- **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`.

- **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**—Specify which language is used in the portal: the user’s browser locale setting, with a fallback to another language if a browser locale is not available. Or force the portal to always use one language.

•

## Login 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 > Login Page Settings**.

Use these settings to define the login experience for users (guests, sponsors or employees as applicable), the parameters for failed login attempts, and AUP information for this page.

Field	Usage Guidelines
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. You can specify the time between attempts after this number of failed logins is reached in <b>Time between login attempts when rate limiting</b> .
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 <b>Maximum failed login attempts before rate limiting</b> .
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 <b>Login</b> 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 <b>Include an AUP on page</b> is enabled.  Ensure that the user has read the AUP completely. The <b>Accept</b> button activates only after the user has scrolled to the end of the AUP.

### Acceptable Use Policy (AUP) 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 > Acceptable Use Policy (AUP) Page Settings**.

Use these settings to define the AUP experience for the users (guests, sponsors or employees as applicable).

Field	Usage Guidelines
Include an AUP page	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 <b>Accept</b> button activates only after the user has scrolled to the end of the AUP.

Field	Usage Guidelines
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 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.

Field	Usage Guidelines
Include a Post-Login Banner page	Display additional information after the users successfully log in and before they are granted network access.

### 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**.

Field	Usage Guidelines
Allow internal users to change password	<p>Allow employees to change their passwords after they log into the My Devices portal.</p> <p>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.</p>

### 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 94: Manage Device Settings for My Devices Portals**

Field	Usage Guidelines
Lost	<p>For all devices.</p> <p>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.</p>
Reinstate	<p>For all devices.</p> <p>This action reinstates a blacklisted, lost or stolen device and resets its 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.</p> <p>If you want to prevent employees reinstating devices that you have blacklisted, do not enable this option in the My Devices portal.</p>
Delete	<p>For all devices.</p> <p>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.</p> <p>To define the maximum number of personal devices that employees can register using either the BYOD or My Devices portals, choose <b>Administration &gt; Device Portal Management &gt; Settings &gt; Employee Registered Devices</b>.</p> <p>To permanently delete the device from the Cisco ISE database, choose <b>Administration &gt; Identity Management &gt; Identities &gt; Endpoints</b>.</p>
Stolen	<p>For all devices.</p> <p>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.</p>

Field	Usage Guidelines
Device lock	<p>For MDM enrolled devices only.</p> <p>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.</p> <p>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.</p>
Unenroll	<p>For MDM enrolled devices only.</p> <p>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.</p>
Full wipe	<p>For MDM enrolled devices only.</p> <p>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.</p>

### 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.

### 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).

Field	Usage Guidelines
Include a Support Information Page	Display a link to an information page, such as <b>Contact Us</b> , on all enabled pages for the portal.
MAC address	Include the MAC address of the device on the Support Information page.

Field	Usage Guidelines
IP address	Include the IP address of the device on the Support Information page.
Browser user agent	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.
Policy server	Include the IP address of the ISE Policy Service Node (PSN) that is serving this portal on the Support Information page.
Failure code	If available, include the corresponding number from the log message catalog. You can access and view the message catalog by navigating to <b>Administration &gt; System &gt; Logging &gt; Message Catalog</b> .
Hide field	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 <b>Failure code</b> , even if it is selected.
Display label with no value	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 <b>Failure code</b> , even if it is blank.
Display label with default value	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 <b>Failure code</b> will display as <b>Not Available</b> .







## Guest Access User Interface Reference

- [Guest Portal Settings, page 755](#)
- [Sponsor Portal Application Settings, page 775](#)
- [Global Settings, page 781](#)

### Guest Portal Settings

#### Portal Identification Settings

The navigation path for these settings is **Guest Access > Configure > Guest Portals or Sponsor Portals > Create, Edit or Duplicate > Guest Portals or Sponsor Portals Settings and Customization**.

Use these settings to identify the portal and select the language files to be used for all the portal pages.

Field	Usage Guidelines
Portal Name	<p>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.</p> <p>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.</p>
Description	Optional.

Field	Usage Guidelines
Portal test URL	<p>A system-generated URL displays as a link after you click <b>Save</b>. Use it to test the portal.</p> <p>Click the link to open a new browser tab that displays the URL for this portal that is being served by a Policy Services Node (PSN) with Policy Services turned on. If Policy Services are not turned on, the PSN will not serve web pages for any portals other than the Admin portal.</p> <p><b>Note</b> 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.</p>
Language File	<p>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.</p> <p>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.</p> <p>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.</p>

## Portal Settings for Hotspot Guest Portals

The navigation path for these settings is **Guest Access > Configure > 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 change this page. If you do change 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 will display.

- **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 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 is used to match Certificate Subject Name / Alternate Subject Name.
- **Certificate group tag**—Select the group tag of the certificate group 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 additional 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 additional 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.
- **CoA Types**
  - CoA Reauthenticate: Causes the NAD to reauthenticate the guest.
  - CoA Terminate: Issues a Change of Authorization (CoA) Terminate to remove the suspended guests from the network.




---

**Note** If you chose CoA-Terminate(Admin-Reset), it could take 10-20 seconds before the user is redirected to the portal. This could cause timeout issues, resulting in incorrect Hotspot flow.

---




---

**Note** The VLAN DHCP Release Page Settings section is editable only when the CoA reauthenticate type is selected.

---

- **Display Language**—Specify which language is used in the portal: the user's browser locale setting, with a fallback to another language if a browser locale is not available. Or force the portal to always use one language.

## Acceptable Use Policy (AUP) Page Settings for Hotspot Guest Portals

The navigation path for this page is **Guest Access > Configure > Guest 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).

Field	Usage Guidelines
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 <b>Accept</b> button activates only after the user has scrolled to the end of the AUP.

## Post-Access Banner Page Settings for Hotspot Portals

The navigation path for this page is **Guest Access > Configure > 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.

Field	Usage Guidelines
Include a Post-Access Banner page	Display additional information after the guests are successfully authenticated and before they are granted network access.

## Portal Settings for Credentialed Guest Portals

The navigation path for these settings is: **Guest Access > Configure > 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 ISE and were using Port values outside this range, they are honored until you make any change to this page. If you do change this page, you must 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.

- **Allowed interfaces**—Select the PSN interfaces where this portal can run. 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.
  - The Ethernet interfaces must use IP addresses on different subnets.
  - The interfaces you enable here must be available on all the PSNs that are running portals, 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. If the interface IP is not the same as the domain, then configure **ip host x.x.x.x yyy.domain.com** in the ISE CLI to map your interface IP to FQDN in the certificate.
- **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, LDAP Directory.
 

Cisco ISE includes a default sponsor Identity Source Sequence for sponsor portals, Sponsor\_Portal\_Sequence.
- **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 additional 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**—Specify which language is used in the portal: the user's browser locale setting, with a fallback to another language if a browser locale is not available. Or force the portal to always use one language.

### Portal Configuration Rules

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:
  - 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**.

## Login Page Settings for Credentialed Guest Portals

The navigation path for this page is: **Guest Access > Configure > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Login Page Settings**.

Use these settings to define the login experience for users (guests, sponsors or employees as applicable), the parameters for failed login attempts, and AUP information for this page.

Field	Usage Guidelines
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. You can specify the time between attempts after this number of failed logins is reached in <b>Time between login attempts when rate limiting</b> .
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 <b>Maximum failed login attempts before rate limiting</b> .
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.

Field	Usage Guidelines
Require acceptance	Require users to accept an AUP before their account is fully enabled. The <b>Login</b> 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 <b>Include an AUP on page</b> is enabled.  Ensure that the user has read the AUP completely. The <b>Accept</b> button activates only after the user has scrolled to the end of the AUP.
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 <b>Self-Registration Page Settings</b> and <b>Self-Registration Success Page Settings</b> .  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 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.

## Self-Registration Page Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access > Configure > 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 need to provide on the Self-Registration form.

Field	Usage Guidelines
Assign self-registered guests to guest type	Choose the guest type to which all the self-registered guests using this portal should be assigned.
Account valid for	Specify the duration for the account in days, hours, or minutes after which the account will expire unless you or the sponsor extend the account duration in the Sponsor portal.

Field	Usage Guidelines
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 / Required	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 <b>SMS Service Provider</b> and <b>Person being Visited</b> to gather important information from self-registering guests.
Guests can choose from these locations to set their time zone	<p>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, etc.)</p> <p>If you only provided one location, it is automatically assigned as the default location and does not display in the portal for guests to view. Additionally, <b>Location</b> is disabled in the list of <b>Fields to include</b>.</p>
SMS Service Provider	Display SMS providers 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 to minimize expenses for your company.
Guests can choose from these SMS providers	<p>Select the SMS providers that should display on the Self-Registration form.</p> <p>If you only selected one as the default SMS provider for the guest to use, it will not display on the Self-Registration form.</p>
Custom Fields	Select additional information that you would like collect 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.



Field	Usage Guidelines
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 their account is fully enabled. The <b>Login</b> 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	<p>This option displays only if <b>Include an AUP on page</b> is enabled.</p> <p>Ensure that the user has read the AUP completely. The <b>Accept</b> button activates only after the user has scrolled to the end of the AUP.</p>
Only allow guests with an email address from	<p>Specify the whitelisted email address domains from which the self-registering guests can enter in <b>Email Address</b> and successfully receive their account credentials; for example, cisco.com, example.com.</p> <p>In this example, if the guests entered <i>myname@cisco.com</i> as their email address, after successful account creation, they receive their login credentials. However, if they entered <i>myname@hotmail.com</i> (or any other address not from cisco.com or example.com), no account is created and they do not get credentials.</p> <p>Leaving this field blank allows registration from any domain, unless there are blacklist domains listed in <b>Do not allow guests with email address from</b>.</p>
Do not allow guests with an email address from	<p>Specify the blacklisted email address domains from which the self-registering guests cannot enter in <b>Email Address</b> and successfully receive their account credentials; for example, cisco.com, example.com.</p> <p>In this example, if the guests entered <i>myname@cisco.com</i> as their email address, no account is created and they do not get credentials.</p>

Field	Usage Guidelines
Require self-registered guests to be approved	<p>Specify that the self-registering guests using this portal require approval from a sponsor before receiving their guest credentials.</p> <p>Then specify one of the options under <b>After registration submission, direct guest to</b> in this page:</p> <ul style="list-style-type: none"> <li>• Self-Registration Success page</li> <li>• Login page with instructions about how to obtain login credentials</li> <li>• URL</li> </ul> <p>If enabled, you should also enable one or both: <b>Email</b> or <b>SMS</b> under <b>Send credential notification upon approval using</b> in this page.</p> <p>Enabling Require self-registered guests to be approved enables the following extra configuration fields, which have the following attributes:</p> <p>Approve/Deny Link Settings—Additional settings allow you to configure:</p> <ul style="list-style-type: none"> <li>• <b>Links are valid for</b>, number of days.</li> <li>• Require approver to enter a username and password for authentication—Authenticate sponsors based on the following ordered list of sponsor portals</li> <li>• Authenticate sponsors based on the following ordered list of sponsor portals—If there are multiple sponsors that can approve this account, then chose the portal that the sponsor must log on to in order to approve the account.</li> </ul>

Field	Usage Guidelines
Email approval request to	<p>If you select:</p> <ul style="list-style-type: none"> <li>• <b>sponsor email addresses listed below</b>, enter the email addresses of sponsors designated as approvers, or an email address or a mailer to which ALL guest approval requests should be sent.</li> <li>• <b>person being visited</b>, the <b>Person being visited</b> and <b>Required</b> options in Fields to include will also be enabled (if they were previously disabled). These fields will be displayed on the Self-Registration form requesting this information from the self-registering guests.</li> </ul> <p>These persons will receive an email notification stating that self-registering guests require approval.</p>
Self-Registration Success page	<p>Direct successfully self-registered guests to the Self-Registration Success page, which displays the fields and messages you have specified in <b>Self Registration Success Page Settings</b>.</p> <p>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 in this page.</p> <p>If you enabled <b>Allow guests to log in directly from the Self-Registration Success page</b> in <b>Self-Registration Success Page Settings</b>, 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.</p>

Field	Usage Guidelines
Login page with instructions about how to obtain login credentials	<p>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."</p> <p>To customize the default message, click on the <b>Portal Page Customization</b> tab and select <b>Self-Registration Page Settings</b>.</p> <p>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 in this page.</p>
URL	<p>Direct successfully self-registered guests to the specified URL while waiting for their account credentials to be delivered.</p> <p>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 in this page.</p>
Email	<p>Choose email as the option by which successfully self-registered guests receive their login credential information. If you choose this option, <b>Email address</b> becomes a required field in the list of <b>Fields to include</b> and you can no longer disable this option.</p>
SMS	<p>Choose SMS as the option by which successfully self-registered guests receive their login credential information. If you choose this option, <b>SMS Service Provider</b> becomes a required field in the list of <b>Fields to include</b> and you can no longer disable this option.</p>

## Self Registration Success Page Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access > Configure > 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.

Field	Usage Guidelines
Include this information on the Self-Registration Success page	<p>Check the fields that you want to display for the successfully self-registered guests on the Self-Registration Success page.</p> <p>If sponsor approval of the guest is not required, check <b>Username</b> and <b>Password</b> 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.</p>
Allow guest to send information to self using	Check the options by which the successfully self-registered guest can send credential information to themselves: <b>Print</b> , <b>Email</b> , or <b>SMS</b> .
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 their account is fully enabled. The <b>Login</b> 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	<p>This field displays if you chose the <b>AUP on page</b> option.</p> <p>Ensure that the user has read the AUP completely. The <b>Accept</b> button activates only after the user has scrolled to the end of the AUP.</p>
Allow guests to log in directly from the Self-Registration Success page	Display a <b>Login</b> 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).

## Acceptable Use Policy (AUP) Page Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access > Configure > Guest 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).

Field	Usage Guidelines
Include an AUP page	Display your company's network-usage terms and conditions on a separate page to the user.

Field	Usage Guidelines
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 <b>Skip AUP for employees</b> .
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 <b>Use different AUP for employees</b> .
Require scrolling to end of AUP	Ensure that the user has read the AUP completely. The <b>Accept</b> 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.

## Guest Change Password Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access > Configure > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Guest Change Password Settings**.

Use this setting to require all guests to change their passwords after they first log in.

Field	Usage Guidelines
Require guest to change password at first login	<p>Require guests to change the password after they first log in.</p> <p>If a guest loses their login credentials after they log in and change their password, sponsors can only reset the guest's password back to a random password.</p> <p>To require internal users using a guest portal to change their password upon their next login, choose <b>Administration &gt; Identity Management &gt; Identities &gt; Users</b>. Select the specific internal user from the Network Access Users list and enable the change password check box.</p>

## Guest Device Registration Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access > Configure > 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 **Guest Access > Configure > Guest Types**.

Field	Usage Guidelines
Automatically register guest devices	<p>Automatically create an endpoint for the device from which the guest is accessing this portal. The endpoint will be added to the endpoint identity group specified for this portal and is subject to the identity group's purge policy.</p> <p>An authorization rule can now be created to allow access to endpoints in that identity group, so that web authentication is no longer required.</p> <p>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 <b>Guest Access &gt; Configure &gt; Guest Types</b> to change the maximum number of devices with which a guest can register.</p>
Allow guests to register devices	<p>Guests can register their devices manually by providing a name, description and MAC address. The MAC address is associated with an endpoint identity group.</p> <p>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.</p>

## BYOD Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access > Configure > 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.

Field	Usage Guidelines
Allow employees to use personal devices on the network	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).
Endpoint identity group	Choose an endpoint identity group to track guest devices. Cisco ISE provides the <b>GuestEndpoints</b> endpoint identity group to use as a default. You can also create additional endpoint identity groups if you choose to not use the default.
Purge endpoints in this identity group when they reach ___ days	<p>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.</p> <p>If changes are made to the Endpoint Purge Policy based on other policy conditions, this setting is no longer available for use.</p>
Allow employees to choose to get guest access only	Let employees access your guest network and avoid additional provisioning and registration that may be required to access your corporate network.
Display Device ID field during registration	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 .



Field	Usage Guidelines
Originating URL	<p>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.</p> <p>For Windows, MAC and Android devices, control is given to the Self-Provisioning Wizard app, which performs the provisioning. Therefore, these devices are not redirected to the originating URL. However, iOS (dot1X) and unsupported devices (that are allowed network access) will be redirected to this URL.</p>
Success page	Display a page indicating that the device registration was successful.
URL	After successfully authenticating to the network, redirect the user's browser to the specified URL, such as your company's website.

## Post-Login Banner Page Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access > Configure > 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.

Field	Usage Guidelines
Include a Post-Login Banner page	Display additional information after the users successfully log in and before they are granted network access.

## Guest Device Compliance Settings for Credentialed Guest Portals

The navigation path for this page is **Guest Access > Configure > Guest 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.

Field	Usage Guidelines
Require guest device compliance	<p>Route guests to the Client Provisioning page and require them to first download the posture agent. This enables posture policies for guests, such as checking for virus protection software and so on.</p> <p>If the guest is an employee using the Credentialed Guest portals to access the network and:</p> <ul style="list-style-type: none"> <li>• If you enabled <b>Allow employees to use personal devices on the network</b> in the <b>BYOD Settings</b>, the employee is redirected to the BYOD flow and will not undergo client provisioning.</li> <li>• If you enabled both <b>Allow employees to use personal devices on the network</b> and <b>Allow employees to choose to get guest access only</b> in the <b>BYOD Settings</b>, and the employee chooses guest access, they are routed to the Client Provisioning page.</li> </ul>

## VLAN DHCP Release Page Settings for Guest Portals

The navigation path for this page is **Guest Access > Configure > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > VLAN DHCP Release Page Settings**.

Use these settings to enable the release and renewal of the guest device IP address.

Field	Usage Guidelines
Enable VLAN DHCP release	<p>Use to refresh the IP address for Windows or Mac OS devices after a VLAN change in both wired and wireless environments for a guest.</p> <p>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 once the new VLAN access is in place. 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.</p> <p>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 <b>Renew Lease</b> button.</p>
Delay to release __ seconds	<p>Enter the delay to release time. It should be brief 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.</p>
Delay to CoA __ seconds	<p>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.</p>
Delay to renew __ seconds	<p>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.</p>

## Authentication Success Settings for Guest Portals

The navigation path for this page is **Guest Access > Configure > Guest Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Authentication Success Settings**.

Use these settings to 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.

For Windows, MAC and Android devices, control is given to the Self-Provisioning Wizard app, which performs the provisioning. Therefore, these devices are not redirected to the originating URL. However, iOS (dot1X) and unsupported devices (that are allowed network access) will be 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 **Guest Access > Configure > 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).

Field	Usage Guidelines
Include a Support Information Page	Display a link to an information page, such as <b>Contact Us</b> , on all enabled pages for the portal.
MAC address	Include the MAC address of the device on the Support Information page.
IP address	Include the IP address of the device on the Support Information page.
Browser user agent	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.
Policy server	Include the IP address of the ISE Policy Service Node (PSN) that is serving this portal on the Support Information page.
Failure code	If available, include the corresponding number from the log message catalog. You can access and view the message catalog by navigating to <b>Administration &gt; System &gt; Logging &gt; Message Catalog</b> .

Field	Usage Guidelines
Hide field	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 <b>Failure code</b> , even if it is selected.
Display label with no value	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 <b>Failure code</b> , even if it is blank.
Display label with default value	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 <b>Failure code</b> will display as <b>Not Available</b> .

## Sponsor Portal Application Settings

### Portal Identification Settings

The navigation path for these settings is **Guest Access > Configure > Guest Portals or Sponsor Portals > Create, Edit or Duplicate > Guest Portals or Sponsor Portals Settings and Customization**.

Use these settings to identify the portal and select the language files to be used for all the portal pages.

Field	Usage Guidelines
Portal Name	<p>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.</p> <p>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.</p>
Description	Optional.

Field	Usage Guidelines
Portal test URL	<p>A system-generated URL displays as a link after you click <b>Save</b>. Use it to test the portal.</p> <p>Click the link to open a new browser tab that displays the URL for this portal that is being served by a Policy Services Node (PSN) with Policy Services turned on. If Policy Services are not turned on, the PSN will not serve web pages for any portals other than the Admin portal.</p> <p><b>Note</b> 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.</p>
Language File	<p>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.</p> <p>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.</p> <p>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.</p>

## 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 change this page. If you do change 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 will display.

- **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 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 is used to match Certificate Subject Name / Alternate Subject Name.
- **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, LDAP Directory.
 

Cisco ISE includes a default sponsor Identity Source Sequence for sponsor portals, Sponsor\_Portal\_Sequence.
- **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**—Specify which language is used in the portal: the user's browser locale setting, with a fallback to another language if a browser locale is not available. Or force the portal to always use one language.

## Login Settings for Sponsor Portals

The navigation path for this page is **Guest Access > Configure > Sponsor Portals > Create, Edit or Duplicate > Portal Behavior and Flow Settings > Login Page Settings**.

Use these settings to define the login experience for users (guests, sponsors or employees as applicable), the parameters for failed login attempts, and AUP information for this page.

**Table 95: Login Page Settings for Sponsor Portals**

Field	Usage Guidelines
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. You can specify the time between attempts after this number of failed logins is reached in <b>Time between login attempts when rate limiting</b> .
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 <b>Maximum failed login attempts before rate limiting</b> .
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 their account is fully enabled. The <b>Login</b> 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 <b>Include an AUP on page</b> is enabled.  Ensure that the user has read the AUP completely. The <b>Accept</b> button activates only after the user has scrolled to the end of the AUP.

## Acceptable Use Policy (AUP) Settings for Sponsor Portals

The navigation path for this page is **Guest Access > Configure > 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).

Field	Usage Guidelines
Include an AUP page	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 <b>Accept</b> 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.



Field	Usage Guidelines
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.

## Sponsor Change Password Settings for Sponsor Portals

The navigation path for this page is **Guest Access > Configure > 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**.

Field	Usage Guidelines
Allow sponsors to change their own passwords	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.

## Post-Login Banner Settings for Sponsor Portals

The navigation path for this page is **Guest Access > Configure > 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.

Field	Usage Guidelines
Include a Post-Login Banner page	Display additional information after the users successfully log in and before they are granted network access.

## Support Information Page Settings for Sponsor Portals

The navigation path for this page is **Guest Access > Configure > 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).

Field	Usage Guidelines
Include a Support Information Page	Display a link to an information page, such as <b>Contact Us</b> , on all enabled pages for the portal.
MAC address	Include the MAC address of the device on the Support Information page.
IP address	Include the IP address of the device on the Support Information page.
Browser user agent	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.
Policy server	Include the IP address of the ISE Policy Service Node (PSN) that is serving this portal on the Support Information page.
Failure code	If available, include the corresponding number from the log message catalog. You can access and view the message catalog by navigating to <b>Administration &gt; System &gt; Logging &gt; Message Catalog</b> .
Hide field	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 <b>Failure code</b> , even if it is selected.
Display label with no value	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 <b>Failure code</b> , even if it is blank.
Display label with default value	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 <b>Failure code</b> will display as <b>Not Available</b> .

## Notify Guests Customization for Sponsor Portals

The navigation path for these settings is **Guest Access > Configure > 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 **Guest Access > Configure > 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 327.
- **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 328.
- **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 329.
- **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 329.
- **Guest Username Policy**—Configure how guest user names are created. For more information, see [Set the Guest Username Policy](#), on page 332 and [Rules for Guest Password Policies](#), on page 330.

- **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 331.
- **SMS Gateway Settings**—Define SMS gateways that will deliver SMS notifications to guests and sponsors. For more information, see [Configure SMS Gateways to Send SMS Notifications to Guests](#), on page 333.

## Guest Type Settings

The navigation path for these settings is **Guest Access > Configure > 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.

Field	Usage Guidelines
Guest type name	Provide a name (from 1-256 characters) that distinguishes this Guest Type from the default Guest Types and others that you create.
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, etc.
Language File	Export or Import the language file to use for portals using this Guest Type.
Collect Additional Data	Select custom fields to collect additional information from Guests.  Custom fields are managed on <b>Guest Access &gt; Settings &gt; Custom Fields</b> .
Maximum Access Time—Account Duration Starts	If you selected <b>From first login</b> , the account start time is assigned when the guest user first logs in to the guest portal. The end time is assigned the specified duration time plus the start time. If the guest user never logs in, the account remains in the Awaiting first login state until the account is removed by the <b>Endpoint Purge</b> settings.  If you selected <b>From sponsor-specified date</b> , 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 this setting, your changes will not apply to existing Guest accounts created using this Guest Type.  Value ranges from 1 to 999.

Field	Usage Guidelines
Allow access only on these days and times	<p>Enter the time ranges and select the days of the week to specify when this Guest Type can access the network. If this guest type remains connected outside these time parameters, they will be logged off. The time ranges are related to the time zones defined by the locations assigned to the guests using this Guest Type.</p> <p>Click the + and - for adding and deleting restricted access times.</p>
Configure guest account Purge Policy	<p>You can schedule an endpoint purge job. The endpoint purge schedule is enabled by default and Cisco ISE deletes endpoints that are older than 30 days. Refer to the <a href="#">Endpoints Purge Settings</a> section for more information.</p>
Login Options—Maximum simultaneous logins	<p>Enter the maximum number of user sessions that this Guest Type can have running concurrently.</p>
When guest exceeds limit	<p>When you select <b>Maximum simultaneous logins</b>, you also must also select the action to take when a user connects after that limit is reached.</p> <p><b>When the guest exceeds limit</b></p> <ul style="list-style-type: none"> <li>• <b>Disconnect the oldest connection</b></li> <li>• <b>Disconnect the newest connection</b> <ul style="list-style-type: none"> <li>◦ <b>Redirect user to a portal page showing an error message:</b> 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 &gt; Error Messages tab.</li> </ul> </li> </ul>
Maximum devices guests can register	<p>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 will only affect newly created Guest accounts.</p>

Field	Usage Guidelines
Allow guest to bypass the Guest portal	<p>Allows users to bypass the credentialed Guest captive portal (web authentication page) and access the network by providing credentials to wired and wireless (dot1x) supplicants or VPN clients. Guest accounts go to Active state bypassing the Awaiting Initial Login state and the AUP page, even if it is required.</p> <p>If you do not enable this setting, users must first log in through the credentialed Guest captive portal before they will be able to access other parts of the network.</p>
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 in advance of the expiration.
View messages in	Specify the language to use when displaying email or SMS notifications as you set them up.
Email	Select email as the method used for account expiry notification.
Use customization from	Select email customization from another portal.
Messages	Enter the the text to use for account expiry notification.
Copy text from	Reuse email text that you created for another Guest Type for account expiry notification.
Send test email to me at	Ensure that the email notification displays as it should by sending it to your email address.
SMS	Select text (SMS) as the method used for account expiry notification.
Messages	Enter the the text to use for account expiry notification.
Copy text from	Reuse text messages that you created for another Guest Type.
Send test SMS to me at	Ensure that the text notification displays as it should by sending it to your cell phone.

Field	Usage Guidelines
These sponsor groups can create this guest type	<p>Select which sponsor groups can create Guest accounts with this Guest Type.</p> <p>If you want to disable use of this Guest Type, do not assign it to any sponsor group. If you want to discontinue use of this Guest Type, delete the sponsor groups listed.</p>

## Sponsor Group Settings

The navigation path for these settings is **Guest Access > Configure > 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.

- **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.

- **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 **Guest Access > Configure > Sponsor Portal > Page Customization > Create Accounts > Guest Types > Settings**. Check **Hide guest type if only one is available to sponsor** to enable this option.

- **Configure Guest Types**

—If the guest type you need is not available, click **Guest Access > Configure > Guest Types** and create a new guest type or edit an existing one.

- **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**

- **View guests' passwords**—For guest accounts that they can manage, allow the sponsor to view the passwords.

If the guest has changed the password, the sponsor can no longer view it; unless it was reset by the sponsor to a random password generated by Cisco ISE.

**Note**

If this option is disabled for a sponsor group, the members of that group cannot send email and SMS notifications regarding the login credentials (guest password) for the guest accounts that they manage.

- **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.
- **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.
- **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.
- **Reinstate suspended guest accounts**—For guest accounts that they can manage, allow the sponsor to reinstate suspended accounts.
- **Approve requests from self-registering guests**—For guest accounts that they can manage, allow the sponsor to approve self-registering guests when they receive an email requesting their approval.
- **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.





## Web Portals Customization Reference

---

- [Portal Pages Titles, Content and Labels Character Limits](#), page 789
- [Portal Customization](#), page 791
- [HTML Support for a Portal Language File](#), page 792
- [Custom Guest Notifications](#), page 801

### 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 Guest portals, choose **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization > Pages**.
- For Sponsor portals, choose **Guest Access > Configure > Sponsor Portals > Edit > Portal Page Customization > Pages**.
- 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.

<b>Field Category</b>	<b>Fields</b>	<b>Field Labels: Minimum Characters</b>	<b>Field Labels: Maximum Characters</b>	<b>Field Input Values: Minimum Characters</b>	<b>Field Input Values: Maximum Characters</b>
Common page elements	Banner title				256
	Footer elements			0	2000
	Browser Page Title			0	256
	Instructional Text			0	2000
	Content Title			0	256
	Optional Content 1			0	2000
	Optional Content 2			0	2000
	Button labels	0	64		
	Check box labels	0	64		
	Tab labels	0	64		
	Link labels	0	256		
AUP	AUP Text			0	50,000
Message text	Message text (displayed on page)			0	2000
	Message text (displayed in pop-up window)			0	256
Field labels	All fields labels	0	256		
Field input (general)	Field input in general (see special cases below)			0	256
Field input (special cases)	Access Code field			1	20
	Registration Code field			1	20
	Username fields			1	64

Field Category	Fields	Field Labels: Minimum Characters	Field Labels: Maximum Characters	Field Input Values: Minimum Characters	Field Input Values: Maximum Characters
	Password fields			1	256
	Phone Number field			0	64
	Device ID field			12	17

## 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.

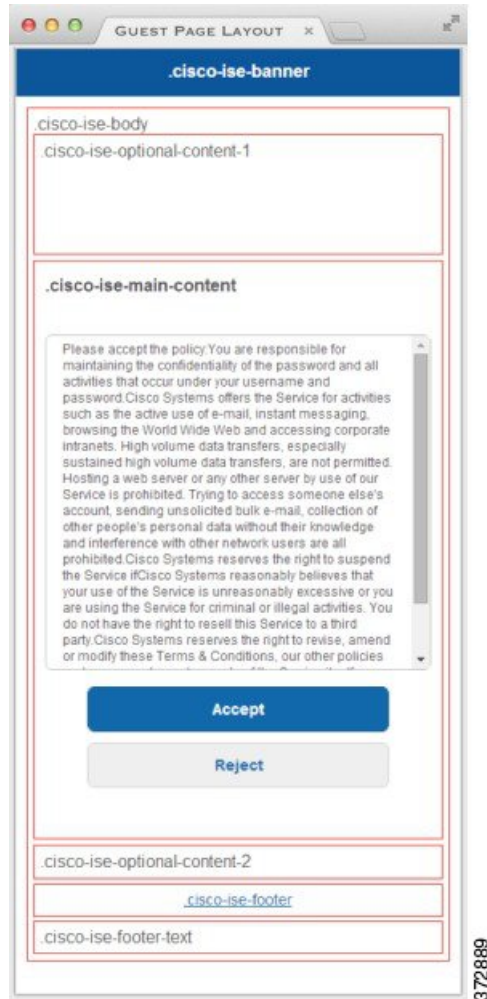
### CSS Classes and Descriptions for End-User Portals Page Layout

Use these CSS classes to define and modify the page layout of the Cisco ISE end-user web portals.

CSS Class Name	Description
cisco-ise-banner	Includes logos, banner image, and banner text. On the Sponsor and My Devices portals, this class also contains buttons that can activate a context menu. For example, the menu can bring up a pop-up window with options to <b>Log Out</b> , <b>Change Password</b> , and so on.
cisco-ise-body	Contains all page elements that are not part of the banner.
cisco-ise-optional-content-1	Empty by default. You can add text, links, and HTML and Javascript code.
cisco-ise-main-content	Includes the main contents of the portal page, such as instructional text, action buttons, and the cisco-ise-footer container.
cisco-ise-optional-content-2	Empty by default. You can add text, links, and HTML and Javascript code.
cisco-ise-footer	Part of the footer, it is a placeholder for links such as <b>Contact Support</b> and online <b>Help</b> .

CSS Class Name	Description
cisco-ise-footer-text	Empty by default. It is a placeholder for anything that you want to display at the bottom of the portal page, such as a copyright notice or a disclaimer.

**Figure 54: CSS Classes Used in the End-User Portal Page Layout**



## 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\_2
- key.guest.ui\_byod\_install\_optional\_content\_2
- key.guest.ui\_byod\_reg\_optional\_content\_1
- 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\_welcome\_instruction\_message
- 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

## 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\_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 **Guest Access > Configure > 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\_contact\_optional\_content\_2
- key.guest.ui\_contact\_optional\_content\_1
- key.guest.ui\_byod\_install\_ios\_instruction\_message
- key.guest.ui\_changepwd\_instruction\_message
- key.guest.ui\_client\_provision\_posture\_check\_compliant\_message
- key.guest.ui\_aup\_instruction\_message
- key.guest.ui\_changepwd\_optional\_content\_2
- key.guest.ui\_changepwd\_optional\_content\_1
- key.guest.ui\_self\_reg\_results\_optional\_content\_2
- key.guest.ui\_self\_reg\_results\_optional\_content\_1
- key.guest.ui\_device\_reg\_instruction\_message
- key.guest.ui\_byod\_welcome\_renew\_cert\_message
- key.guest.ui\_vlan\_execute\_message
- key.guest.ui\_byod\_install\_android\_instruction\_message
- key.guest.ui\_client\_provision\_posture\_check\_non\_compliant\_message
- key.guest.ui\_byod\_install\_instruction\_message
- key.guest.ui\_device\_reg\_max\_reached\_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\_aup\_employee\_text
- key.guest.ui\_client\_provision\_agent\_installed\_instructions\_without\_java\_message
- key.guest.ui\_success\_message
- key.guest.ui\_byod\_welcome\_optional\_content\_1
- key.guest.ui\_byod\_welcome\_optional\_content\_2
- key.guest.ui\_self\_reg\_optional\_content\_2

- key.guest.ui\_self\_reg\_optional\_content\_1
- key.guest.ui\_byod\_reg\_limit\_message
- key.guest.notification\_credentials\_print\_body
- key.guest.ui\_byod\_reg\_content\_message
- key.guest.ui\_client\_provision\_agent\_installation\_message
- 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 **Guest Access > Configure > 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\_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.




---

**Note** This is not a complete list of the dictionary keys in the files.

---

- key.mdm.ui\_contact\_instruction\_message
- key.mdm.ui\_mdm\_enrollment\_after\_message
- key.mdm.ui\_error\_optional\_content\_2
- key.mdm.ui\_error\_optional\_content\_1
- key.mdm.ui\_mdm\_enroll\_optional\_content\_1
- key.mdm.ui\_mdm\_enroll\_optional\_content\_1
- key.mdm.ui\_mdm\_enroll\_optional\_content\_2
- key.mdm.ui\_mdm\_enroll\_instruction\_message
- key.mdm.ui\_error\_instruction\_message
- key.mdm.ui\_mdm\_enrollment\_link\_message
- key.mdm.ui\_mdm\_not\_reachable\_message
- key.mdm.ui\_contact\_optional\_content\_2
- key.mdm.ui\_mdm\_continue\_message
- key.mdm.ui\_contact\_optional\_content\_1

## 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.

---

- key.mydevices.ui\_add\_optional\_content\_1
- key.mydevices.ui\_add\_optional\_content\_2
- key.mydevices.ui\_post\_access\_instruction\_message
- key.mydevices.ui\_edit\_instruction\_message
- key.mydevices.ui\_contact\_optional\_content\_2
- key.mydevices.ui\_contact\_optional\_content\_1

- key.mydevices.ui\_changepwd\_optional\_content\_1
- key.mydevices.ui\_changepwd\_optional\_content\_2
- key.mydevices.ui\_post\_access\_message
- 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

## 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 **Guest Access > Configure > 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.



### 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
- key.sponsor.ui\_home\_instruction\_message
- key.sponsor.ui\_post\_access\_instruction\_message
- key.sponsor.notification\_credentials\_print\_body
- key.sponsor.ui\_aup\_sponsor\_text
- key.sponsor.ui\_create\_accounts\_access\_info\_instruction\_message
- key.sponsor.ui\_login\_instruction\_message
- key.sponsor.notification\_credentials\_email\_body
- key.sponsor.ui\_create\_known\_instruction\_message
- key.sponsor.ui\_create\_import\_instruction\_message
- key.sponsor.ui\_suspend\_account\_instruction\_message
- key.sponsor.ui\_post\_access\_message
- key.sponsor.ui\_login\_optional\_content\_2
- key.sponsor.ui\_login\_optional\_content\_1
- key.sponsor.notification\_credentials\_email\_password\_body
- key.sponsor.ui\_contact\_optional\_content\_2
- key.sponsor.ui\_contact\_optional\_content\_1
- key.sponsor.ui\_login\_aup\_text
- key.sponsor.ui\_changepwd\_instruction\_message
- key.sponsor.ui\_create\_accounts\_guest\_type\_instruction\_message
- key.sponsor.ui\_changepwd\_optional\_content\_1
- key.sponsor.ui\_changepwd\_optional\_content\_2
- key.sponsor.notification\_credentials\_email\_username\_body
- key.sponsor.ui\_aup\_optional\_content\_1
- key.sponsor.ui\_aup\_optional\_content\_2
- key.sponsor.ui\_post\_access\_optional\_content\_1
- key.sponsor.ui\_post\_access\_optional\_content\_2
- key.sponsor.ui\_contact\_instruction\_message

## Custom Guest Notifications

Within in each portal, you can customize the email, SMS text messages, or printed notifications that guests receive.

## List of Variables for Portal Pages Customization

The navigation paths for these portal page text boxes are:

- For Guest portals, choose **Guest Access > Configure > Guest Portals > Edit > Portal Page Customization > Pages**.
- For Sponsor portals, choose **Guest Access > Configure > 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 96: List of Variables for Guest Portals**

Display Name	Substitute with Variable Name
Access code Use to provide an access code to guests using either email, text or print notifications.	ui_access_code
BYOD IOS SSID Use to specify the network that a device should connect to after on-boarding in a dual SSID flow.	ui_byod_success_ios_ssid
Client Provisioning Agent Type Use to specify the currently configured agent in the client provisioning policy, such as the AnyConnect agent or the NAC agent.	ui_client_provision_agent_type
Client Provisioning Agent URL Use to specify the download URL for the posture agent.	ui_client_provision_agent_url
Client Provisioning agent install minutes 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.	ui_client_provision_install_agent_mins
Company	ui_company



<b>Display Name</b>	<b>Substitute with Variable Name</b>
Email address	ui_email_address
End date and time	ui_end_date_time
First name	ui_first_name
Last name	ui_last_name
Location name	ui_location_name
Maximum registered devices	ui_max_reg_devices
Maximum simultaneous logins	ui_max_siml_login
Password	ui_password
Person being visited (email)	ui_person_visited
Phone number	ui_phone_number
Reason for visit	ui_reason_visit
SMS Provider	ui_sms_provider
SSID Use to specify the wireless network that a guest can use to connect to the network.	ui_ssid
Start date and time	ui_start_date_time
Time left	ui_time_left
Username	ui_user_name

**Table 97: List of Variables for Sponsor Portals**

<b>Display Name</b>	<b>Substitute with Variable Name</b>
Guest - Company	ui_guest_company
Guest - Email address	ui_guest_email_address
Guest - End date and time	ui_guest_end_date_time
Guest - First name	ui_guest_first_name
Guest - Last name	ui_guest_last_name

Display Name	Substitute with Variable Name
Guest - Location name	ui_guest_location_name
Guest - Maximum registered devices	ui_guest_max_reg_devices
Guest - Maximum simultaneous logins	ui_guest_max_siml_login
Guest - Password	ui_guest_password
Guest - Person being visited (email)	ui_guest_person_visited
Guest - Phone number	ui_guest_phone_number
Guest - Reason for visit	ui_guest_reason_visit
Guest - SMS Provider	ui_guest_sms_provider
Guest - SSID Use to specify the wireless network that a guest can use to connect to the network.	ui_guest_ssid
Guest - Start date and time	ui_guest_start_date_time
Guest - Time left	ui_guest_time_left
Guest - Username	ui_guest_user_name
Username Use to specify the username of the user logged into the portal.	ui_sponsor_user_name
Use to display "From" in the Guest Access Information page.	ui_from_label
Use to display "First Login" in the Guest Access Information page.	ui_first_login_text
Use to display guest account notification message if the access time starts at First Login.	ui_notification_first_login_text
Dynamic variable that represents the account duration in email notifications.	ui_access_duration
Dynamic variable to display an account that is no longer available. For Start-End accounts, the date is the End date and for From-First-Login account, the date is the account creation date plus the purge duration days.	ui_account_purge_date

Display Name	Substitute with Variable Name
Use to restrict the sponsor from changing the guest type from From First Login to Start-End or vice versa, if the guest user has logged in at least once in the past. Displayed in the General Sponsor Portal Messages.	ui_guest_type_change_ffl_startend_not_allowed_error ui_guest_type_change_startend_ffl_not_allowed_error

**Table 98: List of Variables for MDM Portals**

Display Name	Substitute with Variable Name
MDM - Vendor Name	ui_mdm_vendor_name

**Table 99: List of Variables for My Devices Portals**

Display Name	Substitute with Variable Name
MyDevices - Login Failure Rate Limit	\$user_login_failure_rate_limit\$
MyDevices - Max Devices to Register	ui_max_register_devices
MyDevices - User Name Use to specify the username of the user logged into the portal.	\$session_username\$





## Policy User Interface Reference

- [Authentication, page 807](#)
- [Authorization Policy Settings, page 810](#)
- [Endpoint Profiling Policies Settings, page 811](#)
- [Dictionaries, page 814](#)
- [Conditions, page 816](#)
- [Results, page 829](#)

### Authentication

This section describes the authentication policy page, which allows you to configure simple and rule-based authentication policies.

#### Simple Authentication Policy Configuration Settings

The following table describes the fields in the simple authentication policy page, which allows you to configure simple authentication policies. The navigation path for this page is: **Policy > Authentication**.

**Table 100: Simple Authentication Policy Configuration Settings**

Fields	Usage Guidelines
Network Access Service	Choose an allowed protocol that you have already created.
Identity Source	Choose the identity source that you want to use for authentication. You can also choose an identity source sequence if you have configured it.  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.

Fields	Usage Guidelines
Options	<p>Define a further course of action for authentication failure, user not found, or process failure events. You can choose one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Reject</b>—A reject response is sent.</li> <li>• <b>Drop</b>—No response is sent.</li> <li>• <b>Continue</b>—Cisco ISE proceeds with the authorization policy.</li> </ul>

## Rule-Based Authentication Policy Configuration Settings

The following table describes the fields in the rule-based authentication policy page, which allows you to configure simple authentication policies. The navigation path for this page is: **Policy > Authentication > Rule-Based**.

**Table 101: Rule-Based Authentication Policy Configuration Settings**

Fields	Usage Guidelines
Status	<p>Choose the status of this policy. It can be one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Enabled</b>—This policy condition is active.</li> <li>• <b>Disabled</b>—This policy condition is inactive and will not be evaluated.</li> <li>• <b>Monitor Only</b>—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. 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.</li> </ul>
Standard Rule	Enter a name for this policy and select condition and allowed protocol.
Conditions	<p>Click the plus [+] sign to expand the Conditions anchored overlay, and click the minus [-] sign, or click outside the anchored overlay to close it:</p> <ul style="list-style-type: none"> <li>• <b>Select Existing Condition from Library or Create New Condition (Advanced Option)</b></li> <li>• <b>Select Existing Condition from Library</b>—You can define an expression by selecting Cisco predefined conditions from the policy elements library.</li> <li>• <b>Create New Condition (Advanced Option)</b>—You can define an expression by selecting attributes from various system or user-defined dictionaries.</li> </ul>

Fields	Usage Guidelines
Select Existing Condition from Library	<p>You can do the following:</p> <ol style="list-style-type: none"> <li data-bbox="675 338 1511 850"> <p>You can choose the predefined conditions that you would have defined for authentication in the policy elements, and then use an AND or OR operator to add multiple conditions.</p> <p>You cannot select certain predefined conditions that contain the following dictionaries or attributes:</p> <ul style="list-style-type: none"> <li data-bbox="753 527 1224 558">• Dictionary "Certificate", with any attribute</li> <li data-bbox="753 575 1406 850"> <ul style="list-style-type: none"> <li data-bbox="753 575 1406 606">• Dictionary "Network Access", with the following attributes: <ul style="list-style-type: none"> <li data-bbox="813 625 1027 657">◦ Device IP Address</li> <li data-bbox="813 674 995 705">◦ ISE Host Name</li> <li data-bbox="813 722 1060 753">◦ NetworkDeviceName</li> <li data-bbox="813 770 919 802">◦ Protocol</li> <li data-bbox="813 819 922 850">◦ UseCase</li> </ul> </li> </ul> </li> </ul> <p>In case such conditions are available, the first entry in the select box will be "Only relevant conditions are selectable".</p> </li> <li data-bbox="675 984 1511 1297"> <p>Click the Action icon to do the following in the subsequent steps:</p> <ul style="list-style-type: none"> <li data-bbox="753 1037 1438 1068">• Add Attribute/Value—You can add ad-hoc attribute/value pairs</li> <li data-bbox="753 1085 1511 1117">• Add Condition from Library—You can add Cisco predefined conditions</li> <li data-bbox="753 1134 1312 1165">• Duplicate—Create a copy of the selected condition</li> <li data-bbox="753 1182 1511 1245">• Add Condition to Library— You can save ad-hoc attribute/value pairs that you create to the policy elements library</li> <li data-bbox="753 1262 1170 1293">• Delete—Delete the selected condition</li> </ul> </li> </ol>
Create New Condition (Advance Option)	<p>You can do the following:</p> <ol style="list-style-type: none"> <li data-bbox="675 1419 1511 1482"> <p>You can add ad-hoc attribute/value pairs to your expression, and then use an AND or OR operator to add multiple conditions.</p> </li> <li data-bbox="675 1499 1511 1845"> <p>Click the Action icon to do the following in the subsequent steps:</p> <ul style="list-style-type: none"> <li data-bbox="753 1551 1438 1583">• Add Attribute/Value—You can add ad-hoc attribute/value pairs</li> <li data-bbox="753 1600 1511 1631">• Add Condition from Library—You can add Cisco predefined conditions</li> <li data-bbox="753 1648 1312 1680">• Duplicate—Create a copy of the selected condition</li> <li data-bbox="753 1696 1511 1759">• Add Condition to Library— You can save ad-hoc attribute/value pairs that you create to the policy elements library</li> <li data-bbox="753 1776 1503 1839">• Delete—Delete the selected condition. Here, you can use the AND or OR operator</li> </ul> </li> </ol>

Fields	Usage Guidelines
Select Network Access	Choose from allowed protocols or RADIUS server sequence.
Arrow Button	Click to define conditions for the identity source selection.
Identity Source Sequence	<p>You can do the following:</p> <ol style="list-style-type: none"> <li>1 Click the action icon in the default identity source row, and click Insert new row above.</li> <li>2 Enter a name for your identity source rule.</li> <li>3 Click the button to define the conditions based on which you want to choose the identity source.</li> <li>4 Choose the identity source sequence or the identity source and the action that you want Cisco ISE to take.</li> </ol>

## Authorization Policy Settings

The following table describes the fields in the authorization policy page, which allows you to configure authorization policies. The navigation path for this page is: **Policy > Authorization**.

**Table 102: Authorization Policy Settings**

Fields	Usage Guidelines
Status	<p>Choose one of the following to enforce the policies:</p> <ul style="list-style-type: none"> <li>• Enabled—This policy condition is active.</li> <li>• Disabled—This policy condition is inactive and will not be evaluated.</li> <li>• 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. 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.</li> </ul>
Rule Name	Enter a name for the Rule Name.
Conditions (identity groups and other conditions)	<p>Choose an identity group from the first drop-down.</p> <p>Choose a condition from the second drop-down.</p> <p>You can either select from the existing conditions or create a new condition.</p>



Fields	Usage Guidelines
Permissions	Choose an authorization profile from the <b>Standard</b> category.

## 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 103: Endpoint Profiling Policies Settings**

Fields	Usage Guidelines
Name	Enter the name of the endpoint profiling policy that you want to create.
Description	Enter the description of the endpoint profiling policy that you want to create.
Policy Enabled	By default, the <b>Policy Enabled</b> 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.
Exception Action	Choose an exception action, which you want to associate with the conditions when defining a rule in the profiling policy.  The default is NONE. The exception actions are defined in the following location: Policy > Policy Elements > Results > Profiling > Exception Actions.
Network Scan (NMAP) Action	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.  The default is NONE. The exception actions are defined in the following location: Policy > Policy Elements > Results > Profiling > Network Scan (NMAP) Actions.
Create an Identity Group for the policy	Check one of the following options to create an endpoint identity group: <ul style="list-style-type: none"> <li>• <b>Yes, create matching Identity Group</b></li> <li>• <b>No, use existing Identity Group hierarchy</b></li> </ul>

Fields	Usage Guidelines
Yes, create matching Identity Group	<p>Choose this option to use an existing profiling policy.</p> <p>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.</p> <p>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.</p>
No, use existing Identity Group hierarchy	<p>Check this check box to assign endpoints to the matching parent endpoint identity group using hierarchical construction of profiling policies and identity groups.</p> <p>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.</p> <p>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,</p> <ul style="list-style-type: none"> <li>• If endpoints match the Cisco-IP-Phone profile, then they are grouped under the Cisco-IP-Phone endpoint identity group.</li> <li>• If endpoints match the Workstation profile, then they are grouped under the Workstation endpoint identity group.</li> </ul> <p>The Cisco-IP-Phone and Workstation endpoint identity groups are associated to the Profiled endpoint identity group in the system.</p>
Parent Policy	<p>Choose a parent profiling policy that are defined in the system to which you want to associate the new endpoint profiling policy.</p> <p>You can choose a parent profiling policy from which you can inherit rules and conditions to its child.</p>
Associated CoA Type	<p>Choose one of the following CoA types that you want to associate with the endpoint profiling policy:</p> <ul style="list-style-type: none"> <li>• No CoA</li> <li>• Port Bounce</li> <li>• Reauth</li> <li>• Global Settings that is applied from the profiler configuration set in Administration &gt; System &gt; Settings &gt; Profiling</li> </ul>

Fields	Usage Guidelines
Rules	<p>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.</p> <p>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.</p>
Conditions	<p>Click the plus [+] sign to expand the Conditions anchored overlay, and click the minus [-] sign, or click outside the anchored overlay to close it.</p> <p>Click <b>Select Existing Condition from Library</b> or <b>Create New Condition (Advanced Option)</b> .</p> <p><b>Select Existing Condition from Library</b>---You can define an expression by selecting Cisco predefined conditions from the policy elements library.</p> <p><b>Create New Condition (Advanced Option)</b>---You can define an expression by selecting attributes from various system or user-defined dictionaries.</p> <p>You can associate one of the following with the profiling conditions:</p> <ul style="list-style-type: none"> <li>• An integer value for the certainty factor for each condition</li> <li>• Either an exception action or a network scan action for that condition</li> </ul> <p>Choose one of the following predefined settings to associate with the profiling condition:</p> <ul style="list-style-type: none"> <li>• <b>Certainty Factor Increases</b>—Enter the certainty value for each rule, which can be added for all the matching rules with respect to the overall classification.</li> <li>• <b>Take Exception Action</b>—Triggers an exception action that is configured in the Exception Action field for this endpoint profiling policy.</li> <li>• <b>Take Network Scan Action</b>—Triggers a network scan action that is configured in the Network Scan (NMAP) Action field for this endpoint profiling policy.</li> </ul>

Fields	Usage Guidelines
Select Existing Condition from Library	<p>You can do the following:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Click the Action icon to do the following in the subsequent steps: <ul style="list-style-type: none"> <li>◦ Add Attribute/Value—You can add ad-hoc attribute/value pairs</li> <li>◦ Add Condition from Library—You can add Cisco predefined conditions</li> <li>◦ Duplicate—Create a copy of the selected condition</li> <li>◦ Add Condition to Library— You can save ad-hoc attribute/value pairs that you create to the policy elements library</li> <li>◦ Delete—Delete the selected condition.</li> </ul> </li> </ul>
Create New Condition (Advance Option)	<p>You can do the following:</p> <ul style="list-style-type: none"> <li>• You can add ad-hoc attribute/value pairs to your expression, and then use an AND or OR operator to add multiple conditions.</li> <li>• Click the Action icon to do the following in the subsequent steps: <ul style="list-style-type: none"> <li>◦ Add Attribute/Value—You can add ad-hoc attribute/value pairs</li> <li>◦ Add Condition from Library—You can add Cisco predefined conditions</li> <li>◦ Duplicate—Create a copy of the selected condition</li> <li>◦ Add Condition to Library— You can save ad-hoc attribute/value pairs that you create to the policy elements library</li> <li>◦ Delete—Delete the selected condition. Here, you can use the AND or OR operator</li> </ul> </li> </ul>

## 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 104: RADIUS Vendor Dictionary Attribute Settings**

Fields	Usage Guidelines
Attribute Name	Enter the vendor specific attribute name for the selected RADIUS vendor.
Description	Enter an optional description for the vendor specific attribute.
Internal Name	Enter the name for the vendor specific attribute that refers to it internally in the database.
Data Type	Choose one of the following data types for the vendor specific attribute: <ul style="list-style-type: none"> <li>• STRING</li> <li>• OCTET_STRING</li> <li>• UNIT32</li> <li>• UNIT64</li> <li>• IPV4</li> </ul>
Enable MAC option	<p>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.</p> <p>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.</p>
Direction	Choose one of the options that applies to RADIUS messages:
ID	Enter the vendor attribute ID. The valid range is 0 to 255.
Allow Tagging	<p>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.</p> <p>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.</p>
Allow multiple instances of this attribute in a profile	Check this check box when you want multiple instances of this RADIUS vendor specific attribute in profiles.

## 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 105: Profiler Condition Settings**

Fields	Usage Guidelines
Name	Name of the profiler condition.
Description	Description of the profiler condition.
Type	Choose any one of the predefined types.
Attribute Name	Choose an attribute on which to base the profiler condition.
Operator	Choose an operator.
Attribute Value	Enter the value for the attribute that you have chosen. For Attribute Names that contain pre-defined Attribute Values, this option displays a drop-down list with the pre-defined values, and you can choose a value.
System Type	Profiling conditions can be any one of the following types: <ul style="list-style-type: none"> <li>• Cisco Provided—Profiling conditions that are provided by Cisco ISE when deployed are identified as Cisco Provided. You cannot edit or delete them from the system.</li> <li>• Administrator Created—Profiling conditions that you create as an administrator of Cisco ISE are identified as Administrator Created.</li> </ul>

### Posture Conditions 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 106: File Condition Settings**

<b>Fields</b>	<b>Usage Guidelines</b>
Name	Enter the name of the file condition.
Description	Enter a description for the file condition.
File Path	<p>Choose one of the predefined settings:</p> <ul style="list-style-type: none"> <li>• <b>ABSOLUTE_PATH</b>—Checks the file in the fully qualified path of the file. For example, C:\&lt;directory&gt;\file name. For other settings, enter only the file name.</li> <li>• <b>SYSTEM_32</b>—Checks the file in the C:\WINDOWS\system32 directory. Enter the file name.</li> <li>• <b>SYSTEM_DRIVE</b>—Checks the file in the C:\ drive. Enter the file name.</li> <li>• <b>SYSTEM_PROGRAMS</b>—Checks the file in the C:\Program Files. Enter the file name.</li> <li>• <b>SYSTEM_ROOT</b>—Checks the file in the root path for Windows system. Enter the file name.</li> </ul>
File Type	<p>Choose one of the predefined settings:</p> <ul style="list-style-type: none"> <li>• <b>FileExistence</b>—Checks whether a file exists on the system.</li> <li>• <b>FileDate</b>—Checks whether a file with a particular file-created or file-modified date exists on the system.</li> <li>• <b>FileVersion</b>—Checks whether a particular version of a file exists on the system.</li> </ul>
File Date Type	(Available only if you select <b>FileDate</b> as the File Type) Choose a file data type.
File Operator/Operator	<p>The File Operator options change according to the settings you select in the File Type. Choose the settings appropriately:</p> <p>FileExistence</p> <ul style="list-style-type: none"> <li>• Exists</li> <li>• DoesNotExist</li> </ul> <p>FileDate</p> <ul style="list-style-type: none"> <li>• EarlierThan</li> <li>• LaterThan</li> <li>• EqualTo</li> </ul> <p>FileVersion</p> <ul style="list-style-type: none"> <li>• EarlierThan</li> <li>• LaterThan</li> <li>• EqualTo</li> </ul>

Fields	Usage Guidelines
Date and Time	(Available only if you select <b>FileDate</b> as the File Type) Enter the date and time of the client system in mm/dd/yyyy and hh:mm:ss format.
File Version	(Available only if you have selected <b>FileVersion</b> as the File Type) Enter the version of the file to be checked.
Operating System	Select the operating system to which the file condition should be applied.

**Table 107: File Condition Settings**

Fields	Usage Guidelines for Windows OS	Usage Guidelines for Mac OSX
Name	Enter the name of the file condition.	Enter the name of the file condition.
Description	Enter a description for the file condition.	Enter a description for the file condition.
Operating System	Select any Windows operating system to which the file condition should be applied.	Select any Mac OSX to which the file condition should be applied.
File Path	<p>Choose one of the predefined settings:</p> <ul style="list-style-type: none"> <li>• <b>ABSOLUTE_PATH</b>—Checks the file in the fully qualified path of the file. For example, C:\&lt;directory&gt;\file name. For other settings, enter only the file name.</li> <li>• <b>SYSTEM_32</b>—Checks the file in the C:\WINDOWS\system32 directory. Enter the file name.</li> <li>• <b>SYSTEM_DRIVE</b>—Checks the file in the C:\ drive. Enter the file name.</li> <li>• <b>SYSTEM_PROGRAMS</b>—Checks the file in the C:\Program Files. Enter the file name.</li> <li>• <b>SYSTEM_ROOT</b>—Checks the file in the root path for Windows system. Enter the file name.</li> </ul>	<p>Choose one of the predefined settings:</p> <ul style="list-style-type: none"> <li>• <b>Root</b>—Checks the file in the root (/) directory.</li> <li>• <b>Home</b>—Checks the file in the home (~) directory.</li> </ul>



Fields	Usage Guidelines for Windows OS	Usage Guidelines for Mac OSX
File Type	Choose one of the predefined settings: <ul style="list-style-type: none"> <li>• <b>FileDate</b>—Checks whether a file with a particular file-created or file-modified date exists on the system.</li> <li>• <b>FileExistence</b>—Checks whether a file exists on the system.</li> <li>• <b>FileVersion</b>—Checks whether a particular version of a file exists on the system.</li> <li>• <b>CRC32</b>—Checks the data integrity of a file.</li> </ul>	Choose one of the predefined settings: <ul style="list-style-type: none"> <li>• <b>FileDate</b>—Checks whether a file with a particular file-created or file-modified date exists on the system.</li> <li>• <b>FileExistence</b>—Checks whether a file exists on the system.</li> <li>• <b>CRC32</b>—Checks the data integrity of a file.</li> </ul>
File Date Type	(Available only if you select <b>FileDate</b> as the File Type) Choose <b>Creation Date</b> or <b>Modification Date</b> .	(Available only if you select <b>FileDate</b> as the File Type) Choose <b>Creation Date</b> or <b>Modification Date</b> .
File Operator/Operator	The File Operator options change according to the settings you select in the File Type. Choose the settings appropriately: <p>FileDate</p> <ul style="list-style-type: none"> <li>• EarlierThan</li> <li>• LaterThan</li> <li>• EqualTo</li> </ul> <p>FileExistence</p> <ul style="list-style-type: none"> <li>• Exists</li> <li>• DoesNotExist</li> </ul> <p>FileVersion</p> <ul style="list-style-type: none"> <li>• EarlierThan</li> <li>• LaterThan</li> <li>• EqualTo</li> </ul> <p>CRC32</p> <ul style="list-style-type: none"> <li>• File CRC Data, for example, you can enter a checksum value of 0x3c37fec3. The checksum value should start with 0x, a hexadecimal integer.</li> </ul>	The File Operator options change according to the settings you select in the File Type. Choose the settings appropriately: <p>FileDate</p> <ul style="list-style-type: none"> <li>• EarlierThan</li> <li>• LaterThan</li> <li>• EqualTo</li> </ul> <p>FileExistence</p> <ul style="list-style-type: none"> <li>• Exists</li> <li>• DoesNotExist</li> </ul> <p>CRC32</p> <ul style="list-style-type: none"> <li>• File CRC Data, for example, you can enter a checksum value of 0x3c37fec3. The checksum value should start with 0x, a hexadecimal integer.</li> </ul>

Fields	Usage Guidelines for Windows OS	Usage Guidelines for Mac OSX
Date and Time	(Available only if you select <b>FileDate</b> as the File Type) Enter the date and time of the client system in mm/dd/yyyy and hh:mm:ss format.	(Available only if you select <b>FileDate</b> as the File Type) Enter the date and time of the client system in mm/dd/yyyy and hh:mm:ss format.
File Version	(Available only if you have selected <b>FileVersion</b> as the File Type) Enter the version of the file to be checked.	NA.

### 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 108: Registry Condition Settings**

Fields	Usage Guidelines
Name	Enter the name of the registry condition.
Description	Enter a description for the registry condition.
Registry Type	Choose one of the predefined settings as the registry type.
Registry Root Key	Choose one of the predefined settings as the registry root key.
Sub Key	Enter the sub key without the backslash (“\”) 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
Value Name	(Available only if you select <b>RegistryValue</b> or <b>RegistryValueDefault</b> as the Registry Type) Enter the name of the registry key value to be checked for <b>RegistryValue</b> .  This is the default field for <b>RegistryValueDefault</b> .
Value Data Type	(Available only if you select <b>RegistryValue</b> or <b>RegistryValueDefault</b> as the Registry Type) Choose one of the following settings: <ul style="list-style-type: none"> <li>• <b>Unspecified</b>—Checks whether the registry key value exists or not. This option is available only for <b>RegistryValue</b>.</li> <li>• <b>Number</b>—Checks the specified number in the registry key value</li> <li>• <b>String</b>—Checks the string in the registry key value</li> <li>• <b>Version</b>—Checks the version in the registry key value</li> </ul>

Fields	Usage Guidelines
Value Operator	Choose the settings appropriately.
Value Data	(Available only if you select <b>RegistryValue</b> or <b>RegistryValueDefault</b> as the Registry Type) Enter the value of the registry key according to the data type you have selected in <b>Value Data Type</b> .
Operating System	Select the operating system to which the registry condition should be applied.

### 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 109: Application Condition Settings**

Fields	Usage Guidelines
Name	Enter the name of the application condition.
Description	Enter a description of the application condition.
Process Name	Enter the name of the application to be checked.
Application Operator	Choose the status to be checked.
Operating System	Select the operating system to which the application condition should be applied.

**Table 110: Application Condition Settings**

Fields	Usage Guidelines
Name	Enter the name of the application condition.
Description	Enter a description of the application condition.
Operating System	Select the Windows OS or the MAC OSX to which the application condition should be applied.
Process Name	Enter the name of the application to be checked.
Application Operator	Choose the status to be checked.

## Service Conditions 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 111: Service Conditions Settings**

Fields	Usage Guidelines
Name	Enter a name for the service condition.
Description	Enter a description of the service condition.
Service Name	Enter the name of the service to be checked.
Service Operator	Choose the status to be checked.
Operating System	Select the operating system to which the service condition should be applied.

**Table 112: Service Conditions Settings**

Fields	Usage Guidelines
Name	Enter a name for the service condition.
Description	Enter a description of the service condition.
Operating Systems	Select the operating system to which the service condition should be applied. You can select different versions of the Mac OSX or Windows OS.
Service Name	Enter the name of the service or daemon running as root. The AnyConnect agent uses the command <b>sudo launchctl list</b> to validate the service condition.
Service Operator	Choose the status that you want to check: <ul style="list-style-type: none"> <li>• Windows OS—To check if a service is <b>Running</b> or <b>Not Running</b>.</li> <li>• Mac OSX—To check if a service is <b>Loaded</b> or <b>Unloaded</b>.</li> </ul>

## 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 113: Posture Compound Condition Settings**

Fields	Usage Guidelines
Name	Enter the name of the compound condition that you want to create.
Description	Enter the description of the compound condition that you want to create.
Operating System	Select one or more Windows operating systems. This allow you to associate Windows operating systems to which the condition is applied.
Parentheses ( )	Click the parentheses to combine two simple conditions from the following simple condition types: file, registry, application, and service conditions.
( & )—AND operator (use “&” for an AND operator, without the quotes)	You can use the AND operator (ampersand [ & ]) in a compound condition. For example, enter <b>Condition1 &amp; Condition2</b> .
(   )—OR operator (use “ ” for an OR operator, without the quotes)	You can use the OR operator (horizontal bar [   ]) in a compound condition. For example, enter <b>Condition1 &amp; Condition2</b> .
( ! )—NOT operator (use “!” for a NOT operator, without the quotes)	You can use the NOT operator (exclamation point [ ! ]) in a compound conditions. For example, enter <b>Condition1 &amp; Condition2</b> .
Simple Conditions	<p>Choose from a list of simple conditions of the following types: file, registry, application, and service conditions.</p> <p>You can also create simple conditions of file, registry, application and service conditions from the object selector.</p> <p>Click the quick picker (down arrow) on the <b>Action</b> button to create simple conditions of file, registry, application, and service conditions.</p>

### Antivirus Compound Condition Settings

The following table describes the fields in the AV Compound Conditions page. The navigation path for this page is: **Policy > Policy Elements > Conditions > Posture > AV Compound Condition**.

**Table 114: Antivirus Compound Condition Settings**

Fields	Usage Guidelines
Name	Enter the name of the antivirus compound condition that you want to create.
Description	Enter the description of the antivirus compound condition that you want to create.

Fields	Usage Guidelines
Operating System	Select an operating system to check the installation of an antivirus programs on your client, or check the latest antivirus definition file updates to which the condition is applied.
Vendor	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.
Check Type	Choose whether to check an installation or check the latest definition file update on the client.
Installation	Choose to check only the installation of an antivirus program on the client.
Definition	Choose to check only the latest definition file update of an antivirus product on the client.
Check against latest AV definition file version, if available. (Otherwise check against latest definition file date).	(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.
Allow virus definition file to be (Enabled)	(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.
days older than	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).
latest file date	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.
current system date	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.

Fields	Usage Guidelines
Products for Selected Vendor	<p>Choose an antivirus product from the table. Based on the vendor that you select in the New Anti-virus Compound 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.</p> <p>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.</p>

### 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 115: Antispyware Compound Condition Settings**

Fields	Usage Guidelines
Name	Enter the name of the antispyware compound condition that you want to create.
Description	Enter the description of the antispyware compound condition that you want to create.
Operating System	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.
Vendor	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.
Check Type	Choose if you want to choose a type whether to check an installation, or check the latest definition file update on the client.
Installation	Choose if you want to check only the installation of an antispyware program on the client.
Definition	Choose if you want to check only the latest definition file update of an antispyware product on the client.

Fields	Usage Guidelines
Allow virus definition file to be (Enabled)	<p>Check this check box when you are creating antispyware definition check types, and disabled when creating antispyware installation check types.</p> <p>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.</p> <p>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.</p>
days older than	<p>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).</p>
The current system date	<p>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.</p> <p>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.</p>
Products for Selected Vendor	<p>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.</p> <p>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.</p>

### Dictionary Simple Conditions 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 116: Dictionary Simple Condition Settings**

Fields	Usage Guideline
Name	Enter the name of the dictionary simple condition that you want to create.
Description	Enter the description of the dictionary simple condition that you want to create.
Attribute	Choose an attribute from the dictionary.
Operator	Choose an operator to associate a value to the attribute that you have selected.



Fields	Usage Guideline
Value	Enter a value that you want to associate to the dictionary attribute, or choose a predefined value from the drop-down list.

## 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 117: Dictionary Compound Condition Settings**

Fields	Usage Guidelines
Name	Enter the name of the dictionary compound condition that you want to create.
Description	Enter the description of the dictionary compound condition that you want to create.
Select Existing Condition from Library	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.
Condition Name	Choose dictionary simple conditions that you have already created from the policy elements library.
Expression	The Expression is updated based on your selection from the Condition Name drop-down list.
AND or OR operator	Choose an AND, or an OR operator to logically combine dictionary simple conditions, which can be added from the library. Click the <b>Action</b> icon to do the following: <ul style="list-style-type: none"> <li>• Add Attribute/Value</li> <li>• Add Condition from Library</li> <li>• Delete</li> </ul>
Create New Condition (Advance Option)	Select attributes from various system or user-defined dictionaries. You can also add predefined conditions from the policy elements library in the subsequent steps.
Condition Name	Choose a dictionary simple condition that you have already created.
Expression	From the Expression drop-down list, you can create a dictionary simple condition.
Operator	Choose an operator to associate a value to an attribute.

Fields	Usage Guidelines
Value	Enter a value that you want to associate to the dictionary attribute, or choose a value from the drop-down list.

### 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 118: Patch Management Condition**

Fields	Usage Guidelines
Name	Enter the name of the patch management condition that you want to create.
Description	Enter a description for the patch management condition.
Operating System	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 OSX. You can also select more than one version of an operating system to create the patch management condition.
Vendor Name	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 are retrieved and displayed in the <b>Products for Selected Vendor</b> table. The list in the table changes according to the selected operating system.
Check Type	<p>Select any one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Installation</b>—To check if the selected product is installed on the endpoint. This check type is supported by all vendors.</li> <li>• <b>Enabled</b>—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 <b>Products for Selected Vendor</b> list.</li> <li>• <b>Up to Date</b>—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 <b>Products for Selected Vendor</b> list.</li> </ul> <p>Click the <b>Products for Selected Vendor</b> drop-down arrow, to view the list of products that the vendor you have specified in the <b>Vendor Name</b> 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.</p>

## 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 119: Time and Date Condition Settings**

Fields	Usage Guidelines
Condition Name	Enter the name of the time and date condition.
Description	Enter a description of the time and date condition.
Standard Settings	
All Day	(Default) Set for the entire day.
Specific Hours	Configure hours, minutes, and AM/PM to set a to-and-from time range.
Every Day	(Default) Set for every day.
Specific Days	Configure one or more specific days of the week.
No Start and End Dates	(Default) Set with no start or end date.
Specific Date Range	Configure the month, day, and year to set a to-and-from date range.
Specific Date	Configure a specific month, day, and year.
Exceptions	
Time Range	Configure the hours, minutes, and AM/PM to set a to-and-from time range.
Week Days	Configure one or more specific days of the week.
Date Range	Choose on the following two options: <ul style="list-style-type: none"> <li>• Specific Date Range—Provides drop-down lists you can use to configure a specific to-and-from date range by month, day, and year.</li> <li>• Specific Date—Provides drop-down lists you can use to configure a specific month, day, and year.</li> </ul>

## 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 120: Allowed Protocols**

Fields	Usage Guidelines
Allowed Protocols > Authentication Bypass	
Process Host Lookup	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).
Allowed Protocols > Authentication Protocols	
Allow PAP/ASCII	This option enables PAP/ASCII. PAP uses cleartext passwords (that is, unencrypted passwords) and is the least secure authentication protocol.
Allow CHAP	This option enables CHAP authentication. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with Microsoft Active Directory.
Allow MS-CHAPv1	Check this check box to enable MS-CHAPv1.
Allow MS-CHAPv2	Check this check box to enable MS-CHAPv2.
Allow EAP-MD5	Check this check box to enable EAP-based MD5 password hashed authentication.

Fields	Usage Guidelines
Allow EAP-TLS	<p>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.</p> <p><b>Note</b> EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps to configure certificates.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul>
Allow LEAP	<p>Check this check box to enable Lightweight Extensible Authentication Protocol (LEAP) authentication.</p>
Allow PEAP	<p>Check this check box to enable PEAP authentication protocol and PEAP settings. The default inner method is MS-CHAPv2.</p> <p>When you check the Allow PEAP check box, you can configure the following PEAP inner methods:</p> <ul style="list-style-type: none"> <li>• Allow EAP-MS-CHAPv2—Check this check box to use EAP-MS-CHAPv2 as the inner method. <ul style="list-style-type: none"> <li>◦ Allow Password Change—Check this check box for Cisco ISE to support password changes.</li> <li>◦ Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0 to 3.</li> </ul> </li> <li>• Allow EAP-GTC—Check this check box to use EAP-GTC as the inner method. <ul style="list-style-type: none"> <li>◦ Allow Password Change—Check this check box for Cisco ISE to support password changes.</li> <li>◦ Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0 to 3.</li> </ul> </li> <li>• Allow EAP-TLS—Check this check box to use EAP-TLS as the inner method. <p>Check the <b>Allow authentication of expired certificates to allow certificate renewal in Authorization Policy</b> 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.</p> </li> <li>• 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. To ensure that such PEAP conversations are not dropped, check this check box.</li> </ul>

Fields	Usage Guidelines
Allow EAP-FAST	

Fields	Usage Guidelines
	<p>Check this check box 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.</p> <p>When you check the Allow EAP-FAST check box, you can configure EAP-FAST as the inner method:</p> <ul style="list-style-type: none"> <li>• Allow EAP-MS-CHAPv2 <ul style="list-style-type: none"> <li>◦ Allow Password Change—Check this check box for Cisco ISE to support password changes.</li> <li>◦ Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0-3.</li> </ul> </li> <li>• Allow EAP-GTC <p>Allow Password Change—Check this check box for Cisco ISE to support password changes.</p> <p>Retry Attempts—Specifies how many times Cisco ISE requests user credentials before returning login failure. Valid values are 0-3.</p> </li> <li>• Use PACs—Choose this option to configure Cisco ISE to provision authorization PACs for EAP-FAST clients. Additional PAC options appear.</li> <li>• 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. <p>When you choose this option, you can configure Cisco ISE to perform machine authentication.</p> </li> <li>• Allow EAP-TLS—Check this check box to use EAP-TLS as the inner method. <p>Check the <b>Allow authentication of expired certificates to allow certificate renewal in Authorization Policy</b> 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.</p> </li> <li>• Enable EAP Chaining—Check this check box to enable EAP chaining. <p>EAP chaining allows Cisco ISE to correlate the results of user and machine authentication and apply the appropriate authorization policy using the EAPChainingResult attribute.</p> <p>EAP chaining requires a supplicant that supports EAP chaining on the client device. Cisco ISE supports AnyConnect 4.0. Choose the User and Machine Authentication option in the supplicant.</p> <p>EAP chaining is available when you choose the EAP-FAST protocol (both in PAC based and PAC less mode).</p> <p>For PAC-based authentication, you can use user authorization PAC or machine authorization PAC, or both to skip the inner method.</p> <p>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</p> </li> </ul>

Fields	Usage Guidelines
	<p>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.</p> <p>After you enable EAP chaining, update your authorization policy and add a condition using the NetworkAccess:EapChainingResult attribute and assign appropriate permissions. For example:</p> <ul style="list-style-type: none"> <li>◦ If EapChainingResult equal User and machine both succeeded - Full access</li> <li>◦ If EapChainingResult equal User passed and machine failed - Restricted access</li> <li>◦ If EapChainingResult equal User failed and machine passed - Restricted access</li> <li>◦ If EapChainingResult equal User and machine both failed - Authentication fails. Cisco ISE does not process the authorization policy and sends a reject access message.</li> </ul>
Preferred EAP Protocol	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.

## 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 121: PAC Options**

Fields	Usage Guidelines
Use PAC	

Fields	Usage Guidelines
	<ul style="list-style-type: none"> <li>• 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.</li>   <li>• 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%.</li>   <li>• 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.</li>   <li>• 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. <ul style="list-style-type: none"> <li>◦ 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.</li> </ul> </li>   <li>• 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 details are extracted from the PAC and verified in the Cisco ISE external identity source. Cisco ISE only supports Active Directory as an external identity source for machine authentication. After these details are correctly verified, no further authentication is performed. <p>When you check this option, you can enter a value for the amount of time that a machine PAC is acceptable for use. When Cisco ISE receives an expired machine PAC, it automatically reprovisions the end-user client with a new machine PAC (without waiting for a new machine PAC request from the end-user client).</p> </li>   <li>• Enable Stateless Session Resume—Check this check box for Cisco ISE to provision authorization PACs for EAP-FAST clients and skip phase two of EAP-FAST (default = enabled). <p>Uncheck this check box in the following cases:</p> <ul style="list-style-type: none"> <li>◦ If you do not want Cisco ISE to provision authorization PACs for</li> </ul> </li> </ul>

Fields	Usage Guidelines
	<p>EAP-FAST clients</p> <ul style="list-style-type: none"> <li>◦ To always perform phase two of EAP-FAST</li> </ul> <p>When you check this option, you can enter the authorization period of the user authorization PAC. After this period, the PAC expires. When Cisco ISE receives an expired authorization PAC, it performs phase two EAP-FAST authentication.</p>

## 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 122: Authorization Profile settings**

Fields	Usage Guidelines
Name	Enter a name that identifies the new authorization profile.
Description	Enter a description of the authorization profile.
Access Type	Choose the access type options ( <b>ACCESS_ACCEPT</b> or <b>ACCESS_REJECT</b> ).
Service Template	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.
Common Tasks	
DAACL Name	Check the check box and choose existing downloadable ACL options available (for example, Cisco ISE provides two default values in the drop-down list: <b>PERMIT_ALL_TRAFFIC</b> or <b>DENY_ALL_TRAFFIC</b> ). The list will include all current DAACLs in the local database.
VLAN	<p>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.</p> <p><b>Note</b> 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.</p>

Fields	Usage Guidelines
Voice Domain Permission	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.
Posture Discovery	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=https://ip:8443/guestportal/gateway?sessionId=SessionValueIdValue&action=cpp.
Centralized Web Authentication	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 <b>Default</b> or <b>Manual</b> 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=https://ip:8443/guestportal/gateway?sessionId=SessionValueIdValue&action=cwa.  Check the <b>Static IP/Host Name</b> 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.
Web Redirection (CWA, DRW, MDM, NSP, CPP)	
Auto SmartPort	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.
Filter-ID	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.
Reauthentication	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 <b>RADIUS-Request</b> (a value of 1). Setting this to the RADIUS-Request value maintains connectivity during the reauthentication process.

Fields	Usage Guidelines
MACSec Policy	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: <b>must-secure</b> , <b>should-secure</b> , or <b>must-not-secure</b> . For example, your choice is reflected in the Attributes Details pane as: <code>cisco-av-pair = linksec-policy=must-secure</code> .
NEAT	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: <code>cisco-av-pair = device-traffic-class=switch</code> .
Web Authentication (Local Web Auth)	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 <code>cisco-av-pair = priv-lvl=15</code> and this is reflected in the Attributes Details pane.
Wireless LAN Controller (WLC)	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 <code>rsa-1188</code> , this would be reflected in the Attributes Details pane as: <code>Airespace-ACL-Name = rsa-1188</code> .
ASA VPN	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.
Advanced Attributes Settings	
Dictionaries	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.
Attribute Values	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.  <b>Note</b> 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.
Attributes Details	This pane displays any of the configured attribute values that you set for the Common Tasks and Advanced Attributes.  <b>Note</b> The values displayed in the Attributes Details pane are read-only and cannot be edited or deleted in this pane.

## 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 123: Creating an Exception Action**

Fields	Usage Guidelines
Name	Enter the name of the exception action that you want to create.
Description	Enter the description of the exception action that you want to create.
CoA Action to enforce CoA	Check the <b>CoA Action</b> 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 > System > Settings > Profiling.
Policy Assignment	Click the <b>Policy Assignment</b> 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.
System Type	Exception Actions can be any one of the following types: <ul style="list-style-type: none"> <li>• Cisco Provided—Includes AuthorizationChange, EndpointDelete, and FirstTimeProfile</li> <li>• Administrator Created—Includes that are created by you as an administrator of Cisco ISE.</li> </ul>

## 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 124: File Remediation**

Fields	Usage Guidelines
File Remediation Name	Enter a name for the file remediation. Once created and saved, you cannot edit the name of the file remediation.
File Remediation Description	Enter a description for the file remediation.
Version	Enter the file version.

Fields	Usage Guidelines
File to upload	Click <b>Browse</b> 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.

## 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 125: Link Remediation**

Fields	Usage Guidelines
Link Remediation Name	Enter a name for link remediation.
Link Remediation Description	Enter a description for the link remediation.
Remediation Type	Choose one of the following: <ul style="list-style-type: none"> <li>• <b>Automatic</b>—When selected, you should enter values for the Interval and Retry Count.</li> <li>• <b>Manual</b>—When selected, Retry Count and Interval fields are not editable.</li> </ul>
Retry Count	Enter the number of attempts that clients can try to remediate from the link.
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate from the link after previous attempts.
URL	Enter a valid URL that leads to a remediation page or resource.

## Antivirus 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 126: Antivirus Remediation**

Fields	Usage Guidelines
Name	Enter a name for the antivirus remediation.
Description	Enter a description for the antivirus remediation.

Fields	Usage Guidelines
Remediation Type	Choose one of the following: <ul style="list-style-type: none"> <li>• <b>Automatic</b>—When selected, you should enter values for the Interval and Retry Count.</li> <li>• <b>Manual</b>—When selected, Retry Count and Interval fields are not editable.</li> </ul>
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	Enter the number of attempts that clients can try to update an antivirus definition.
Operating System	Choose one of the following: <ul style="list-style-type: none"> <li>• <b>Windows</b></li> <li>• <b>Macintosh</b>—when selected Remediation Type, Interval, and Retry Count fields are not editable</li> </ul>
AV Vendor Name	Choose the antivirus vendor.

## 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 127: Antispyware Remediation**

Fields	Usage Guidelines
Name	Enter a name for the antispyware remediation.
Description	Enter a description for the antispyware remediation.
Remediation Type	Choose one of the following: <ul style="list-style-type: none"> <li>• <b>Automatic</b>—When selected, you should enter values for the Interval and Retry Count.</li> <li>• <b>Manual</b>—When selected, Retry Count and Interval fields are not editable.</li> </ul>
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	Enter the number of attempts that clients can try to update an antispyware definition.



Fields	Usage Guidelines
Operating System	Choose one of the following: <ul style="list-style-type: none"> <li>• <b>Windows</b></li> <li>• <b>Macintosh</b>—when selected, Remediation Type, Interval, and Retry Count fields are not editable</li> </ul>
AS Vendor Name	Choose the antispyware vendor.

## 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 128: Launch Program Remediation**

Fields	Usage Guidelines
Name	Enter a name for the launch program remediation.
Description	Enter a description for the launch program remediation that you want to create.
Remediation Type	Choose one of the following: <ul style="list-style-type: none"> <li>• <b>Automatic</b>—When selected, you should enter the Retry Count and Interval options.</li> <li>• <b>Manual</b>—When selected, Interval and Retry Count fields are not editable.</li> </ul>
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	Enter the number of attempts that clients can try to launch required programs.
Program Installation Path	From the drop-down list, choose the path where the remediation program has to be installed. <ul style="list-style-type: none"> <li>• <b>ABSOLUTE_PATH</b>—remediation program is installed in the fully qualified path of the file. For example, C:\&lt;directory&gt;\</li> <li>• <b>SYSTEM_32</b>—remediation program is installed in the C:\WINDOWS\system32 directory</li> <li>• <b>SYSTEM_DRIVE</b>—remediation program is installed in the C:\ drive</li> <li>• <b>SYSTEM_PROGRAMS</b>—remediation program is installed in the C:\Program Files</li> <li>• <b>SYSTEM_ROOT</b>—remediation program is installed in the root path of Windows system</li> </ul>

Fields	Usage Guidelines
Program Executable	Enter the name of the remediation program executable, or an installation file.
Program Parameters	Enter required parameters for the remediation programs.
Existing Programs	Existing Programs table displays the installation paths, name of the remediation programs, and parameters if any. <ul style="list-style-type: none"> <li>• Click <b>Add</b> to add remediation programs to the Existing Programs list.</li> <li>• Click the delete icon to remove the remediation programs from the list.</li> </ul>

## 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 129: Windows Update Remediation**

Fields	Usage Guidelines
Name	Enter a name for the Windows update remediation.
Description	Enter a description for the Windows update remediation.
Remediation Type	Choose one of the following: <ul style="list-style-type: none"> <li>• <b>Automatic</b>—When selected, you should enter the Retry Count and Interval options.</li> <li>• <b>Manual</b>—When selected, Interval and Retry Count fields are not editable.</li> </ul>
Interval (in seconds)	Enter the time interval in seconds that clients can try to remediate after previous attempts.
Retry Count	Enter the number of attempts that Windows clients can try for Windows updates.

Fields	Usage Guidelines
Windows Update Setting	<p>Choose from the following:</p> <ul style="list-style-type: none"> <li>• Do not change setting—The Windows Automatic Updates client configuration does not change during or after Windows update remediation.</li> <li>• Notify to download and install—Windows only notifies clients, but does not automatically download, or install them.</li> <li>• Automatically download and notify to install—Windows downloads updates for clients, and notifies clients to install Windows updates.</li> <li>• Automatically download and install—Windows automatically downloads, and installs Windows updates. This is the highly recommended setting for Windows clients.</li> </ul>
Override User's Windows Update setting with administrator's	<p>Check this check box to enforce the administrator-specified setting for Windows Automatic Updates on all the clients during, and after Windows update remediation.</p> <p>If unchecked, the setting enforces the following:</p> <ul style="list-style-type: none"> <li>• The administrator-specified setting only when Automatic Updates are disabled on Windows clients.</li> <li>• The Windows clients-specified setting only when Windows Automatic Updates are enabled on the client.</li> </ul>

## 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 Update Remediation**.

**Table 130: WSUS Remediation**

Fields	Usage Guidelines
Name	Enter a name for the WSUS remediation.
Description	Enter a description for the WSUS remediation.
Remediation Type	<p>Choose from the following:</p> <ul style="list-style-type: none"> <li>• <b>Automatic</b>—The NAC Agents automatically updates Windows clients with the latest WSUS updates.</li> <li>• <b>Manual</b>—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.</li> </ul>

Fields	Usage Guidelines
Interval (in seconds)	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.
Retry Count	Enter the number of attempts that the NAC Agents and web Agents retry to update Windows clients with WSUS updates.
Validate Windows updates using	Choose from the following: <ul style="list-style-type: none"> <li>• <b>Cisco Rules</b>—If you choose this option, you can select custom or preconfigured rules as conditions in the posture requirement</li> <li>• <b>Severity Level</b>—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.</li> </ul>
Windows Updates Severity Level	Choose the severity level: <ul style="list-style-type: none"> <li>• <b>Critical</b>—Installs only critical Windows updates</li> <li>• <b>Express</b>—Installs important and critical Windows updates</li> <li>• <b>Medium</b>—Installs all critical, important, and moderate Windows updates</li> <li>• <b>All</b>—Installs all critical, important, moderate, and low Windows updates</li> </ul> <p><b>Note</b> 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.</p>
Update to latest OS Service Pack	Check this check box to allow WSUS remediation install the latest service pack available for the client's operating system automatically. <p><b>Note</b> The operating system service packs are updated automatically irrespective of the Medium and All severity level options selected in WSUS remediation.</p>
Windows Updates Installation Source	Specifies the source from where you install WSUS updates on Windows clients: <ul style="list-style-type: none"> <li>• <b>Microsoft server</b>—Microsoft-managed WSUS server</li> <li>• <b>Managed server</b>—Locally administered WSUS server</li> </ul>

Fields	Usage Guidelines
Installation Wizard Interface Setting	<p>Allows you to display the installation wizard on the client during WSUS updates:</p> <ul style="list-style-type: none"> <li>• <b>Show UI</b>—Displays the Windows Update Installation Wizard progress on Windows clients. Users must have Administrator privileges on clients to view the installation wizard during WSUS updates.</li> <li>• <b>No UI</b>—Hides the Windows Update Installation Wizard progress on Windows clients.</li> </ul>

## 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 131: Patch Management Remediation**

Fields	Usage Guidelines
Name	Enter a name for the patch management remediation.
Description	Enter a description for the patch management remediation.
Remediation Type	<p>Choose one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Automatic</b>—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.</li> <li>• <b>Manual</b>—(Interval and Retry Count fields are disabled) Non-compliant clients should download and apply the latest patches manually.</li> </ul>
Interval (in seconds)	(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.
Retry Count	(Available only when you select the Automatic remediation type) Enter the number of times that a client can attempt to update critical patches.
Operating System	Windows OS is the only OS that is supported.

Fields	Usage Guidelines
Patch Management Vendor Name	<p>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 <b>Products for Selected Vendor</b> table.</p> <p><b>Note</b> Supported versions of Cisco ISE and AnyConnect:</p> <ul style="list-style-type: none"> <li>• Cisco ISE version 1.4</li> <li>• AnyConnect version 4.1 and later</li> </ul>
Remediation Option	<p>Select any one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Enable</b>—Enables the patch management software, in case it is disabled on the endpoint.</li> <li>• <b>Install Missing Patches</b>—Updates the patch on the endpoint.</li> <li>• <b>Activate Patch Management Software GUI</b>—Displays the patch management software user interface. Follow the instructions on this page to change the software settings or initiate software updates.</li> </ul> <p>Click the <b>Products for Selected Vendor</b> drop-down arrow, to view the list of products that the vendor you have specified in the <b>Patch Management Vendor Name</b> 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 <b>Products for Selected Vendor</b> table changes according to the selected remediation option.</p>

## 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 132: Posture Requirement**

Fields	Usage Guidelines
Name	Enter a name for the requirement.
Operating Systems	<p>Choose an operating system.</p> <p>Click plus [+] to associate more than one operating system to the policy.</p> <p>Click minus [-] to remove the operating system from the policy.</p>

Fields	Usage Guidelines
Conditions	<p>Choose a Condition from the list.</p> <p>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.</p> <p>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.</p> <p>The pr_WSUSRule cannot be viewed in the Compound conditions list page. You can only select the pr_WSUSRule from the Conditions widget.</p>
Remediation Actions	<p>Choose a Remediation from the list.</p> <p>You can also create a remediation action and associate it with the requirement.</p> <p>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 non compliance of clients with messages.</p> <p>The <b>Message Text Only</b> 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.</p>







## Operations User Interface Reference

- [Recent RADIUS Authentications](#), page 851
- [Show Live Sessions](#), page 852
- [Diagnostic Tools](#), page 854

### Recent RADIUS Authentications

The following table describes the fields on the Authentications page, which displays recent RADIUS authentications. The navigation path for this page is: **Operations > Authentications > Show Live Authentication**.

**Table 133: Live Authentications**

Option	Usage Guidelines
Time	Shows the time that the log was received by the monitoring and troubleshooting collection agent. This column is required and cannot be deselected.
Status	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.
Details	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.
Repeat Counter	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
Reset Repeat Counts	Click to reset the Retry options for all the endpoints
Identity	Shows the username that is associated with the authentication.
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.

Option	Usage Guidelines
Endpoint Profile	Shows the type of endpoint that is profiled, for example, profiled to be an iPhone, Android, MacBook, Xbox, and so on.
Authentication Policy	Shows the name of the policy selected for specific authentication.
IP Address	Shows the IP address of the endpoint device.
Network Device	Shows the IP address of the Network Access Device.
Device Port	Shows the port number at which the endpoint is connected.
Authorization Profiles	Shows an authorization profile that was used for authentication.
Identity Group	Shows the identity group that is assigned to the user or endpoint, for which the log was generated.
Posture Status	Shows the status of posture validation and details on the authentication.
Event	Shows the event status.
Failure Reason	Shows a detailed reason for failure, if the authentication failed.
Auth Method	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.
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and the like.
Security Group	Shows the group that is identified by the authentication log.
Server	Indicates the Policy Service from which the log was generated.
Session ID	Shows the session ID.

## Show Live Sessions

The following table describes the fields on the live sessions page, which displays live authentication sessions. The navigation path for this page is: **Operations > Authentications > Show Live Sessions**.

**Table 134: Live Sessions**

<b>Field</b>	<b>Description</b>
Initiated	Shows the timestamp when the authentication session was initiated.
Updated	Shows the timestamp when the session was last updated due to any change, like a CoA action.
Account Session Time	Shows the time span (in seconds) of a user's session.
Session Status	Shows the current status of the endpoint device.
CoA Action	Use this to dynamically change the authorization of an active RADIUS session or disconnect an active RADIUS session.
Repeat Count	Shows the number of times the session has been retried.
Endpoint ID	Shows the unique identifier for an endpoint, usually a MAC or IP address.
Identity	Shows the username of the endpoint device.
IP Address	Shows the IP address of the endpoint device.
Audit Session ID	Shows a unique session identifier provided by NAS.
Account Session ID	Shows a unique ID provided by NAS.
Endpoint Profile	Shows the endpoint profile for the device.
Posture Status	Shows the status of posture validation and details on the authentication.
Security Group	Shows the group that is identified by the authentication log.
Server	Indicates the Policy Service from which the log was generated.
Auth Method	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.
Authentication Protocol	Shows the authentication protocol used, such as Protected Extensible Authentication Protocol (PEAP), Extensible Authentication Protocol (EAP), and the like.
NAS IP Address	Shows IP address of the network devices.
Device Port	Shows the connected port to the network device.
PRA Action	Shows the periodic reassessment action taken on a client after it is successfully postured for compliance on your network.

Field	Description
EPS Status ANC Status	Shows the Endpoint Protection Service Adaptive Network Control status of a device as Quarantine, Unquarantine, or Shutdown.
WLC Roam	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.
Packets In	Shows the number of packets received.
Packets Out	Shows the number of packets sent.
Bytes In	Shows the number of bytes received.
Bytes Out	Shows the number of bytes sent.
Session Source	Shows if the endpoint was authenticated via RADIUS or Identity Mapping.

## 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 135: RADIUS Authentication Troubleshooting Settings**

Option	Usage Guidelines
Username	Enter the username of the user whose authentication you want to troubleshoot.
MAC Address	Enter the MAC address of the device that you want to troubleshoot.
Audit Session ID	Enter the audit session ID that you want to troubleshoot.
NAS IP	Enter the NAS IP address.
NAS Port	Enter the NAS port number.
Authentication Status	Choose the status of your RADIUS authentication.
Failure Reason	Enter the failure reason or click <b>Select</b> to choose a failure reason from a list. Click <b>Clear</b> to clear the failure reason.

Option	Usage Guidelines
Time Range	Select a time range. The RADIUS authentication records that are created during this time range are used.
Start Date-Time	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 <i>mm/dd/yyyy</i> format and time in the <i>hh:mm</i> format.
End Date-Time	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 <i>mm/dd/yyyy</i> format and time in the <i>hh:mm</i> format.
Fetch Number of Records	Choose the number of records that you want to fetch from the drop-down list: 10, 20, 50, 100, 200, or 500.

## 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 136: Execute Network Device Command Settings**

Option	Usage Guidelines
Enter Information	
Network Device IP	Enter the IP address of the network device on which you want to run the command.
Command	Enter the <b>show</b> command.

## 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 137: Evaluate Configuration Validator Settings**

Option	Usage Guidelines
Enter Information	

Option	Usage Guidelines
Network Device IP	Enter the IP address of the network device whose configuration you want to evaluate.
Select the configuration items below that you want to compare against the recommended template.	
AAA	This option is selected by default.
RADIUS	This option is selected by default.
Device Discovery	This option is selected by default.
Logging	This option is selected by default.
Web Authentication	Check this check box to compare the web authentication configuration.
Profiler Configuration	Check this check box to compare the Profiler configuration.
Trustsec	Check this check box if you want to compare Trustsec configuration.
802.1X	Check this check box if you want to compare the 802.1X configuration, and choose one of the available options.

## 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 138: Posture Troubleshooting Settings**

Option	Usage Guidelines
Search and Select a Posture event for troubleshooting	
Username	Enter the username to filter on.
MAC Address	Enter the MAC address to filter on, using format: xx-xx-xx-xx-xx-xx
Posture Status	Select the authentication status to filter on:
Failure Reason	Enter the failure reason or click <b>Select</b> to choose a failure reason from a list. Click <b>Clear</b> to clear the failure reason.
Time Range	Select a time range. The RADIUS authentication records that are created during this time range are used.

Option	Usage Guidelines
Start Date-Time:	(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 <i>mm/dd/yyyy</i> format and time in the <i>hh:mm</i> format.
End Date-Time:	(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 <i>mm/dd/yyyy</i> format and time in the <i>hh:mm</i> format.
Fetch Number of Records	Select the number of records to display: 10, 20, 50, 100, 200, 500
Search Result	
Time	Time of the event
Status	Posture status
Username	User name associated with the event
MAC Address	MAC address of the system
Failure Reason	Failure reason for the event

## 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 139: TCP Dump Settings**

Option	Usage Guidelines
Status	<ul style="list-style-type: none"> <li>• Stopped—the tcpdump utility is not running</li> <li>• Start—Click to start the tcpdump utility monitoring the network.</li> <li>• Stop—Click to stop the tcpdump utility</li> </ul>
Host Name	<p>Choose the name of the host to monitor from the drop-down list.</p> <p><b>Note</b> Inline Posture Nodes are not supported.</p>

Option	Usage Guidelines
Network Interface	Choose the network interface to monitor from the drop-down list. <b>Note</b> 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.
Promiscuous Mode	<ul style="list-style-type: none"> <li>• On—Click to turn on promiscuous mode (default).</li> <li>• Off—Click to turn off promiscuous mode.</li> </ul> <p>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.</p>
Filter	Enter a boolean expression on which to filter. Standard tcpdump filter expressions are supported.
Format	Select a format for the tcpdump file.
Dump File	<p>Displays data on the last dump file, such as the following:</p> <p>Last created on Wed Apr 27 20:42:38 UTC 2011 by admin</p> <pre>File size: 3,744 bytes Format: Raw Packet Data Host Name: Positron Network Interface: GigabitEthernet 0 Promiscuous Mode: On</pre> <ul style="list-style-type: none"> <li>• Download—Click to download the most recent dump file.</li> <li>• Delete—Click to delete the most recent dump file.</li> </ul>

## 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 140: Peer SXP Devices for SXP-IP Mappings**

Option	Usage Guidelines
Peer SXP Devices	
Peer IP Address	IP address of the peer SXP device.
VRF	The VRF instance of the peer device.



Option	Usage Guidelines
Peer SXP Mode	The SXP mode of the peer device; for example, whether it is a speaker or a listener.
Self SXP Mode	The SXP mode of the network device; for example, whether it is a speaker or a listener.
Connection State	The status of the connection.
Common Connection Parameters	
User Common Connection Parameters	<p>Check this check box to enable common connection parameters for all the peer SXP devices.</p> <p><b>Note</b> 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.</p>
Username	Enter the username of the peer SXP device.
Password	Enter the password to gain access to the peer device.
Protocol	<ul style="list-style-type: none"> <li>Choose the protocol.</li> </ul> <p><b>Note</b> Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.</p>
Port	<ul style="list-style-type: none"> <li>Enter the port number. The default port number for Telnet is 23 and SSH is 22.</li> </ul>
Enable Password	Enter the enable password if it is different from your login password.
Same as login password	Check this check box if your enable password is the same as your login password.

## 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 141: IP User SGT**

Option	Usage Guidelines
Enter Information	

Option	Usage Guidelines
Network Device IP	Enter the IP address of the network device.
Filter Results	
Username	Enter the username of the user whose records you want to troubleshoot.
User IP Address	Enter the IP address of the user whose records you want to troubleshoot.
SGT	Enter the user SGT value.

## 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 142: Device SGT Settings**

Option	Usage Guidelines
Enter Information	
Network Device IPs (comma-separated list)	Enter the network device IP addresses (whose device SGT you want to compare with an ISE-assigned device SGT) separated by commas.
Common Connection Parameters	
Use Common Connection Parameters	<p>Select this check box to use the following common connection parameters for comparison:</p> <ul style="list-style-type: none"> <li>• Username—Enter the username of the network device.</li> <li>• Password—Enter the password.</li> <li>• Protocol—Choose the protocol. <ul style="list-style-type: none"> <li><b>Note</b> Telnet is the default option. If you choose SSHv2, SSH connections must be enabled on the network device.</li> </ul> </li> <li>• Port—Enter the port number. The default port number for Telnet is 23 and SSH is 22.</li> </ul>
Enable Password	Enter the enable password if it is different from your login password.
Same as login password	Select this check box if your enable password is the same as your login password.

## 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 143: Progress Details Settings**

Option	Usage Guidelines
Specify Connection Parameters for Network Device a.b.c.d	
Username	Enter the username for logging in to the network device.
Password	Enter the password.
Protocol	Choose the protocol. <b>Note</b> Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.
Port	Enter the port number.
Enable Password	Enter the enable password.
Same As Login Password	Check this check box if the enable password is the same as the login password.
Use Console Server	Select this check box to use the console server.
Console IP Address	(If the Use Console Server check box is selected) Enter the console IP address.
Advanced (Use if there is an "Expect timeout error" or the device has non-standard prompt strings) <b>Note</b> The Advanced options appear only for some of the troubleshooting tools.	
Username Expect String	Enter the string that the network device uses to prompt for username; for example, Username:, Login:, and so on.
Password Expect String	Enter the string that the network device uses to prompt for password; for example, Password:.
Prompt Expect String	Enter the prompt that the network device uses. For example, #, >, and @.
Authentication Failure Expect String	Enter the string that the network device returns when there is an authentication failure; for example, Incorrect password, Login invalid, and so on.

## 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 144: RADIUS Authentication Troubleshooting Results Summary**

Option	Usage Guidelines
Diagnosis and Resolution	
Diagnosis	The diagnosis for the problem is listed here.
Resolution	The steps for resolution of the problem are detailed here.
Troubleshooting Summary	
Summary	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.



## Network Access Flows

---

- [Password-Based Authentication](#), page 863
- [RADIUS Protocol Support in Cisco ISE](#), page 864
- [Network Access for Users](#), page 864

### 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

## 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)

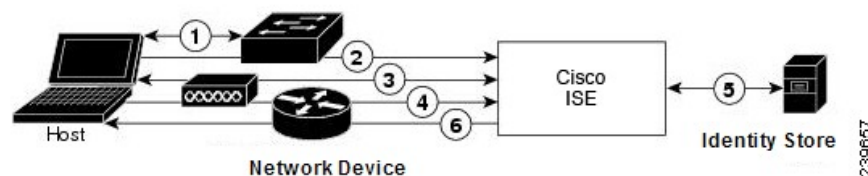
## RADIUS-Based Non-EAP Authentication Flow

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 55: 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
- PEAP/EAP-GTC
- EAP-FAST/EAP-MS-CHAPv2



- EAP-FAST/EAP-GTC

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.

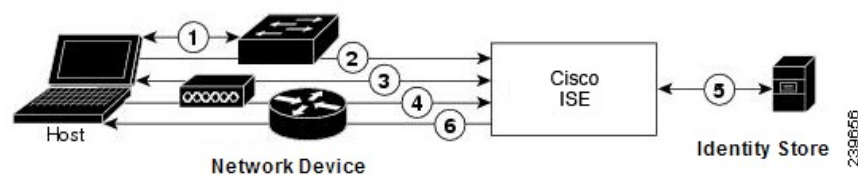
In this way, the host and Cisco ISE indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication.

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 56: 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 acknowledgement 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.

## 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, page 872](#)
- [Local Username and Password Definition for Synthetic RADIUS Transactions, page 872](#)
- [NTP Server Configuration to Ensure Accurate Log and Accounting Timestamps, page 872](#)
- [Command to Enable AAA Functions, page 872](#)
- [RADIUS Server Configuration on the Switch, page 873](#)
- [Configure the Switch to Send RADIUS Accounting Start/Stop to Inline Posture Nodes, page 874](#)
- [Command to Enable RADIUS Change of Authorization \(CoA\), page 874](#)
- [Command to Enable Device Tracking and DHCP Snooping, page 874](#)
- [Command to Enable 802.1X Port-Based Authentication, page 875](#)
- [Command to Enable EAP for Critical Authentications, page 875](#)
- [Command to Throttle AAA Requests Using Recovery Delay, page 875](#)
- [VLAN Definitions Based on Enforcement States, page 875](#)
- [Local \(Default\) ACLs Definition on the Switch, page 876](#)
- [Enable Cisco Trustsec Switch Ports, page 878](#)
- [Command to Enable EPM Logging, page 879](#)
- [Command to Enable SNMP Traps, page 879](#)
- [Command to Enable SNMP v3 Query for Profiling, page 879](#)
- [Command to Enable MAC Notification Traps for Profiler to Collect, page 880](#)

- [RADIUS Idle-Timeout Configuration on the Switch, page 880](#)
- [Wireless LAN Controller Configuration for iOS Supplicant Provisioning, page 880](#)
- [Wireless LAN Controller Support for Apple Devices, page 880](#)
- [Configuring ACLs on the Wireless LAN Controller for MDM Interoperability, page 881](#)

## 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 usernametest-radius key
0 <RADIUS-KEY>

!
radius-server vsa send accounting
!
radius-server vsa send authentication
!
! send RADIUS requests from the MANAGEMENT VLAN

ip radius source-interface <VLAN_number>

```

**Note**


---

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.

---

## Configure the Switch to Send RADIUS Accounting Start/Stop to Inline Posture Nodes

The network access device should be configured to send RADIUS accounting “Start” and “Stop” messages at the beginning and end of a session, respectively, with the remote device’s IP address in those messages to the Inline Posture nodes. The Inline Posture node associates the device IP address to any relevant authorization profiles downloaded over the life of a session. For example, a remote device may have an “unknown-compliance-state” authorization profile at initial login, then switch to a “compliant” authorization profile following CoA (assuming successful device posture assessment).

## 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.



### Note

The first IP helper goes to the DHCP server and the second IP helper sends a copy of the DHCP request to the inline posture node for profiling.

```
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 Cisco Trustsec Switch Ports

To ensure Cisco ISE is able to interoperate with an existing Cisco Trustsec deployment, use the following procedure to ensure that you have enabled all of the functions necessary on the switch.

- 
- 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 Release 12.2(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 **authentication periodic** ! Enable re-authentication via RADIUS Session-Timeout  
**authentication timer reauthenticate server authentication event fail action next-method authentication event server dead action authorize <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):

- Step 11** ! Enable MAC Authentication Bypass (MAB) **mab**  
 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:

**snmp-server community public RO**

**snmp-server trap-source <VLAN\_number>**

## 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

To support Apple iOS-based devices (iPhone/iPad) switching from one SSID to another on the same wireless access point, be sure to 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.

```
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.

## Wireless LAN Controller Support for Apple Devices

Apple devices include the Apple Captive Network Assistant (CNA) feature, which detects captive networks (like the Cisco ISE WebAuth page), but it interferes with the portal redirection required to support guests and personal devices.

You can bypass this feature by enabling the **web-auth captive-bypass** command on the Wireless LAN Controller (WLC):

```
WLC > config network web-auth captive-bypass enable
```

```
Web-auth support for Captive-Bypass will be enabled.
```

```
You must reset system for this setting to take effect.
```

```
WLC > save config
Are you sure you want to save? (y/n) y
Configuration Saved!
WLC >
```

## 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.

- 
- Step 1** Allow all outbound traffic from server to client.
  - Step 2** (Optional) Allow ICMP inbound traffic from client to server for troubleshooting.
  - Step 3** Allow access to MDM server for unregistered and noncompliant devices to download the MDM agent and proceed with compliance checks.
  - Step 4** Allow all inbound traffic from client to server to ISE for Web Portal and supplicant, and certificate provisioning flows.
  - Step 5** Allow inbound DNS traffic from client to server for name resolution.
  - Step 6** Allow inbound DHCP traffic from client to server for IP addresses.
  - Step 7** Deny all inbound traffic from client to server to corporate resources for redirection to ISE (as per your company policy).
  - Step 8** (Optional) Permit the rest of the traffic.
-

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 57: ACLs for Redirecting Nonregistered Device**

General										
Access List Name		NSP-ACL								
Deny Counters		0								
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720	
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227	
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626	
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505	
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864	
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0	
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0	
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4	
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457	
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256	
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310	
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0	
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819	





# CHAPTER 34

## Supported Management Information Bases in Cisco ISE

---

- [IF-MIB, page 883](#)
- [SNMPv2-MIB, page 884](#)
- [IP-MIB, page 884](#)
- [CISCO-CDP-MIB, page 885](#)
- [CISCO-VTP-MIB, page 886](#)
- [CISCO-STACK-MIB, page 886](#)
- [BRIDGE-MIB, page 887](#)
- [OLD-CISCO-INTERFACE-MIB, page 887](#)
- [CISCO-LWAPP-AP-MIB, page 887](#)
- [CISCO-LWAPP-DOT11-CLIENT-MIB, page 889](#)
- [CISCO-AUTH-FRAMEWORK-MIB, page 890](#)
- [EEE8021-PAE-MIB: RFC IEEE 802.1X, page 890](#)
- [HOST-RESOURCES-MIB, page 890](#)
- [LLDP-MIB, page 891](#)

### IF-MIB

**Table 145:**

<b>Object</b>	<b>OID</b>
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2

Object	OID
ifType	1.3.6.1.2.1.2.2.1.3
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8

## SNMPv2-MIB

*Table 146:*

Object	OID
system	1.3.6.1.2.1.1
sysDescr	1.3.6.1.2.1.1.1.0
sysObjectID	1.3.6.1.2.1.1.2.0
sysUpTime	1.3.6.1.2.1.1.3.0
sysContact	1.3.6.1.2.1.1.4.0
sysName	1.3.6.1.2.1.1.5.0
sysLocation	1.3.6.1.2.1.1.6.0
sysServices	1.3.6.1.2.1.1.7.0
sysORLastChange	1.3.6.1.2.1.1.8.0
sysORTable	1.3.6.1.2.1.1.9.0

## IP-MIB

*Table 147:*

Object	OID
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2

Object	OID
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2

## CISCO-CDP-MIB

**Table 148:**

Object	OID
cdpCacheEntry	1.3.6.1.4.1.9.9.23.1.2.1.1
cdpCacheIfIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.1
cdpCacheDeviceIndex	1.3.6.1.4.1.9.9.23.1.2.1.1.2
cdpCacheAddressType	1.3.6.1.4.1.9.9.23.1.2.1.1.3
cdpCacheAddress	1.3.6.1.4.1.9.9.23.1.2.1.1.4
cdpCacheVersion	1.3.6.1.4.1.9.9.23.1.2.1.1.5
cdpCacheDeviceId	1.3.6.1.4.1.9.9.23.1.2.1.1.6
cdpCacheDevicePort	1.3.6.1.4.1.9.9.23.1.2.1.1.7
cdpCachePlatform	1.3.6.1.4.1.9.9.23.1.2.1.1.8
cdpCacheCapabilities	1.3.6.1.4.1.9.9.23.1.2.1.1.9
cdpCacheVTPMgmtDomain	1.3.6.1.4.1.9.9.23.1.2.1.1.10
cdpCacheNativeVLAN	1.3.6.1.4.1.9.9.23.1.2.1.1.11
cdpCacheDuplex	1.3.6.1.4.1.9.9.23.1.2.1.1.12
cdpCacheApplianceID	1.3.6.1.4.1.9.9.23.1.2.1.1.13
cdpCacheVlanID	1.3.6.1.4.1.9.9.23.1.2.1.1.14
cdpCachePowerConsumption	1.3.6.1.4.1.9.9.23.1.2.1.1.15
cdpCacheMTU	1.3.6.1.4.1.9.9.23.1.2.1.1.16
cdpCacheSysName	1.3.6.1.4.1.9.9.23.1.2.1.1.17

Object	OID
cdpCacheSysObjectID	1.3.6.1.4.1.9.9.23.1.2.1.1.18
cdpCachePrimaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.19
cdpCachePrimaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.20
cdpCacheSecondaryMgmtAddrType	1.3.6.1.4.1.9.9.23.1.2.1.1.21
cdpCacheSecondaryMgmtAddr	1.3.6.1.4.1.9.9.23.1.2.1.1.22
cdpCachePhysLocation	1.3.6.1.4.1.9.9.23.1.2.1.1.23
cdpCacheLastChange	1.3.6.1.4.1.9.9.23.1.2.1.1.24

## CISCO-VTP-MIB

*Table 149:*

Object	OID
vtpVlanIfIndex	1.3.6.1.4.1.9.9.46.1.3.1.1.18.1
vtpVlanName	1.3.6.1.4.1.9.9.46.1.3.1.1.4.1
vtpVlanState	1.3.6.1.4.1.9.9.46.1.3.1.1.2.1

## CISCO-STACK-MIB

*Table 150:*

Object	OID
portIfIndex	1.3.6.1.4.1.9.5.1.4.1.1.11
vlanPortVlan	1.3.6.1.4.1.9.5.1.9.3.1.3.1

## BRIDGE-MIB

**Table 151:**

Object	OID
dot1dTpFdbPort	1.3.6.1.2.1.17.4.3.1.2
dot1dBasePortIfIndex	1.3.6.1.2.1.17.1.4.1.2

## OLD-CISCO-INTERFACE-MIB

**Table 152:**

Object	OID
locIfReason	1.3.6.1.4.1.9.2.2.1.1.20

## CISCO-LWAPP-AP-MIB

**Table 153:**

Object	OID
cLApEntry	1.3.6.1.4.1.9.9.513.1.1.1.1
cLApSysMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.1
cLApIfMacAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.2
cLApMaxNumberOfDot11Slots	1.3.6.1.4.1.9.9.513.1.1.1.1.3
cLApEntPhysicalIndex	1.3.6.1.4.1.9.9.513.1.1.1.1.4
cLApName	1.3.6.1.4.1.9.9.513.1.1.1.1.5
cLApUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.6
cLLwappUpTime	1.3.6.1.4.1.9.9.513.1.1.1.1.7
cLLwappJoinTakenTime	1.3.6.1.4.1.9.9.513.1.1.1.1.8
cLApMaxNumberOfEthernetSlots	1.3.6.1.4.1.9.9.513.1.1.1.1.9

Object	OID
cLApPrimaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.10
cLApPrimaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.11
cLApSecondaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.12
cLApSecondaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.13
cLApTertiaryControllerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.14
cLApTertiaryControllerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.15
cLApLastRebootReason	1.3.6.1.4.1.9.9.513.1.1.1.1.16
cLApEncryptionEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.17
cLApFailoverPriority	1.3.6.1.4.1.9.9.513.1.1.1.1.18
cLApPowerStatus	1.3.6.1.4.1.9.9.513.1.1.1.1.19
cLApTelnetEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.20
cLApSshEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.21
cLApPreStdStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.22
cLApPwrInjectorStateEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.23
cLApPwrInjectorSelection	1.3.6.1.4.1.9.9.513.1.1.1.1.24
cLApPwrInjectorSwMacAddr	1.3.6.1.4.1.9.9.513.1.1.1.1.25
cLApWipsEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.26
cLApMonitorModeOptimization	1.3.6.1.4.1.9.9.513.1.1.1.1.27
cLApDomainName	1.3.6.1.4.1.9.9.513.1.1.1.1.28
cLApNameServerAddressType	1.3.6.1.4.1.9.9.513.1.1.1.1.29
cLApNameServerAddress	1.3.6.1.4.1.9.9.513.1.1.1.1.30
cLApAMSDUEnable	1.3.6.1.4.1.9.9.513.1.1.1.1.31
cLApEncryptionSupported	1.3.6.1.4.1.9.9.513.1.1.1.1.32
cLApRogueDetectionEnabled	1.3.6.1.4.1.9.9.513.1.1.1.1.33

## CISCO-LWAPP-DOT11-CLIENT-MIB

**Table 154:**

<b>Object</b>	<b>OID</b>
cldcClientEntry	1.3.6.1.4.1.9.9.599.1.3.1.1
cldcClientMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.1
cldcClientStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.2
cldcClientWlanProfileName	1.3.6.1.4.1.9.9.599.1.3.1.1.3
cldcClientWgbStatus	1.3.6.1.4.1.9.9.599.1.3.1.1.4
cldcClientWgbMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.5
cldcClientProtocol	1.3.6.1.4.1.9.9.599.1.3.1.1.6
cldcAssociationMode	1.3.6.1.4.1.9.9.599.1.3.1.1.7
cldcApMacAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.8
cldcIfType	1.3.6.1.4.1.9.9.599.1.3.1.1.9
cldcClientIPAddress	1.3.6.1.4.1.9.9.599.1.3.1.1.10
cldcClientNacState	1.3.6.1.4.1.9.9.599.1.3.1.1.11
cldcClientQuarantineVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.12
cldcClientAccessVLAN	1.3.6.1.4.1.9.9.599.1.3.1.1.13
cldcClientLoginTime	1.3.6.1.4.1.9.9.599.1.3.1.1.14
cldcClientUpTime	1.3.6.1.4.1.9.9.599.1.3.1.1.15
cldcClientPowerSaveMode	1.3.6.1.4.1.9.9.599.1.3.1.1.16
cldcClientCurrentTxRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.17
cldcClientDataRateSet	1.3.6.1.4.1.9.9.599.1.3.1.1.18

## CISCO-AUTH-FRAMEWORK-MIB

*Table 155:*

Object	OID
cafPortConfigEntry	1.3.6.1.4.1.9.9.656.1.2.1.1
cafSessionClientMacAddress	1.3.6.1.4.1.9.9.656.1.4.1.1.2
cafSessionStatus	1.3.6.1.4.1.9.9.656.1.4.1.1.5
cafSessionDomain	1.3.6.1.4.1.9.9.656.1.4.1.1.6
cafSessionAuthUserName	1.3.6.1.4.1.9.9.656.1.4.1.1.10
cafSessionAuthorizedBy	1.3.6.1.4.1.9.9.656.1.4.1.1.12
cafSessionAuthVlan	1.3.6.1.4.1.9.9.656.1.4.1.1.14

## EEE8021-PAE-MIB: RFC IEEE 802.1X

*Table 156:*

Object	OID
dot1xAuthAuthControlledPortStatus	1.0.8802.1.1.1.1.2.1.1.5
dot1xAuthAuthControlledPortControl	1.0.8802.1.1.1.1.2.1.1.6
dot1xAuthSessionUserName	1.0.8802.1.1.1.1.2.4.1.9

## HOST-RESOURCES-MIB

*Table 157:*

Object	OID
hrDeviceDescr	1.3.6.1.2.1.25.3.2.1.3
hrDeviceStatus	1.3.6.1.2.1.25.3.2.1.5



## LLDP-MIB

**Table 158:**

<b>Object</b>	<b>OID</b>
lldpEntry	1.0.8802.1.1.2.1.4.1.1
lldpTimeMark	1.0.8802.1.1.2.1.4.1.1.1
lldpLocalPortNum	1.0.8802.1.1.2.1.4.1.1.2
lldpIndex	1.0.8802.1.1.2.1.4.1.1.3
lldpChassisIdSubtype	1.0.8802.1.1.2.1.4.1.1.4
lldpChassisId	1.0.8802.1.1.2.1.4.1.1.5
lldpPortIdSubtype	1.0.8802.1.1.2.1.4.1.1.6
lldpPortId	1.0.8802.1.1.2.1.4.1.1.7
lldpPortDescription	1.0.8802.1.1.2.1.4.1.1.8
lldpSystemName	1.0.8802.1.1.2.1.4.1.1.9
lldpSystemDescription	1.0.8802.1.1.2.1.4.1.1.10
lldpCapabilitiesMapSupported	1.0.8802.1.1.2.1.4.1.1.11
lldpCacheCapabilities	1.0.8802.1.1.2.1.4.1.1.12

