



User Guide for Cisco Secure Access Control System 5.8.1

Last Updated: 7/25/17

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

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

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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: 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. (1721R)

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

© 2015 Cisco Systems, Inc. All rights reserved.



Preface	xxi
Audience	xxi
Document Conventions	xxi
Documentation Updates	xxii
Related Documentation	xxii
Obtaining Documentation and Submitting a Service Request	xxiii

CHAPTER 1

Introducing ACS 5.8.1	1-1
Overview of ACS	1-1
ACS Distributed Deployment	1-2
ACS 4.x and 5.8.1 Replication	1-2
ACS Licensing Model	1-3
ACS Management Interfaces	1-3
ACS Web-Based Interface	1-4
ACS Command-Line Interface	1-4
ACS Programmatic Interfaces	1-5
Hardware Models Supported by ACS	1-6

CHAPTER 2

Migrating from ACS 4.x to ACS 5.8.1	2-1
Overview of the Migration Process	2-1
Migration Requirements	2-2
Supported Migration Versions	2-2
Before You Begin	2-2
Downloading Migration Files	2-3
Migrating from ACS 4.x to ACS 5.8.1	2-3
Functionality Mapping from ACS 4.x to ACS 5.8.1	2-4
Common Scenarios in Migration	2-7
Migrating from ACS 4.2 on CSACS 1121 to ACS 5.8.1	2-7
Migrating from ACS 3.x to ACS 5.8.1	2-8
Migrating Data from Other AAA Servers to ACS 5.8.1	2-8

CHAPTER 3

ACS 5.x Policy Model 3-1

- Overview of the ACS 5.x Policy Model 3-1
 - Policy Terminology 3-2
 - Simple Policies 3-3
 - Rule-Based Policies 3-4
 - Types of Policies 3-4
- Access Services 3-5
 - Identity Policy 3-8
 - Group Mapping Policy 3-10
 - Authorization Policy for Device Administration 3-11
- Service Selection Policy 3-12
- Simple Service Selection 3-12
- Rules-Based Service Selection 3-12
 - Access Services and Service Selection Scenarios 3-13
 - First-Match Rule Tables 3-13
- Authorization Profiles for Network Access 3-16
 - Processing Rules with Multiple Authorization Profiles 3-16
- Policies and Identity Attributes 3-17
- Policies and Network Device Groups 3-17
- Example of a Rule-Based Policy 3-18
- Flows for Configuring Services and Policies 3-19

CHAPTER 4

Common Scenarios Using ACS 4-1

- Overview of Device Administration 4-2
 - Session Administration 4-3
 - Command Authorization 4-4
 - TACACS+ Custom Services and Attributes 4-4
- Password-Based Network Access 4-5
 - Overview of Password-Based Network Access 4-5
 - Password-Based Network Access Configuration Flow 4-6
- Certificate-Based Network Access 4-8
 - Overview of Certificate-Based Network Access 4-9
 - Using Certificates in ACS 4-10
- Agentless Network Access 4-12
 - Overview of Agentless Network Access 4-12
 - Host Lookup 4-12
 - Authentication with Call Check 4-14
 - PAP/EAP-MD5 Authentication 4-15

Agentless Network Access Flow	4-15
Adding a Host to an Internal Identity Store	4-16
Configuring an LDAP External Identity Store for Host Lookup	4-17
Configuring an Identity Group for Host Lookup Network Access Requests	4-17
Creating an Access Service for Host Lookup	4-18
VPN Remote Network Access	4-20
Supported Authentication Protocols	4-20
Supported Identity Stores	4-20
Supported VPN Network Access Servers	4-21
Supported VPN Clients	4-21
Configuring VPN Remote Access Service	4-21
ACS and Cisco Security Group Access	4-22
Adding Devices for Security Group Access	4-23
Creating Security Groups	4-23
Creating SGACLs	4-24
Configuring an NDAC Policy	4-24
Configuring EAP-FAST Settings for Security Group Access	4-25
Creating an Access Service for Security Group Access	4-25
Creating an Endpoint Admission Control Policy	4-25
Creating an Egress Policy	4-26
Creating a Default Policy	4-27
RADIUS and TACACS+ Proxy Requests	4-27
RADIUS Attribute Rewrite Operation	4-29
Supported Protocols	4-33
Supported RADIUS Attributes	4-33
TACACS+ Body Encryption	4-34
Connection to TACACS+ Server	4-34
Configuring Proxy Service	4-34
FIPS 140-2 Level 1 Implementation	4-35
Cisco NAC Agent Requirements When FIPS Mode Is Enabled	4-37
Enabling and Disabling IPv6 for Network Interfaces	4-37

CHAPTER 5
Understanding My Workspace 5-1

Welcome Page	5-1
Task Guides	5-2
My Account Page	5-2
Login Banner	5-3
Using the Web Interface	5-4

Accessing the Web Interface	5-4
Understanding the Web Interface	5-6
Importing and Exporting ACS Objects Through the Web Interface	5-19
Supported ACS Objects	5-19
Creating Import Files	5-22
Common Errors	5-25
Concurrency Conflict Errors	5-26
Deletion Errors	5-27
System Failure Errors	5-27
Accessibility	5-28
Display and Readability Features	5-28
Keyboard and Mouse Features	5-28
Obtaining Additional Accessibility Information	5-29

CHAPTER 6

Post-Installation Configuration Tasks	6-1
Configuring Minimal System Setup	6-1
Configuring ACS to Perform System Administration Tasks	6-1
Configuring ACS to Manage Access Policies	6-3
Configuring ACS to Monitor and Troubleshoot Problems in the Network	6-4

CHAPTER 7

Managing Network Resources	7-1
Network Device Groups	7-1
Creating, Duplicating, and Editing Network Device Groups	7-2
Deleting Network Device Groups	7-3
Creating, Duplicating, and Editing Network Device Groups Within a Hierarchy	7-3
Deleting Network Device Groups from a Hierarchy	7-4
Network Devices and AAA Clients	7-5
Viewing and Performing Bulk Operations for Network Devices	7-5
Exporting Network Devices and AAA Clients	7-7
Performing Bulk Operations for Network Resources and Users	7-8
Exporting Network Resources and Users	7-9
Creating, Duplicating, and Editing Network Devices	7-10
Displaying Network Device Properties	7-14
Deleting Network Devices	7-17
Using Single Static IP Addresses That Are Part of IP Subnets and IP Ranges	7-17
Configuring a Default Network Device	7-18
Working with External Proxy Servers	7-19
Creating, Duplicating, and Editing External Proxy Servers	7-20

CHAPTER 8

Deleting External Proxy Servers	7-21
Working with OCSP Services	7-22
Creating, Duplicating, and Editing OCSP Servers	7-23
Deleting OCSP Servers	7-25
Managing Users and Identity Stores	8-1
Overview	8-1
Internal Identity Stores	8-1
External Identity Stores	8-2
Identity Groups	8-3
Certificate-Based Authentication	8-3
Identity Sequences	8-4
Managing Internal Identity Stores	8-4
Authentication Information	8-5
Identity Groups	8-6
Managing Identity Attributes	8-7
Configuring Authentication Settings for Users	8-9
Disabling User Account After <i>N</i> Days of Inactivity	8-12
Creating Internal Users	8-13
Deleting Users from Internal Identity Stores	8-17
Enable and Disable Password Hashing for Internal Users	8-18
Configuring Password Expiry Notification Emails to Users and Administrators	8-19
Viewing and Performing Bulk Operations for Internal Identity Store Users	8-21
Configuring Authentication Settings for Hosts	8-22
Creating Hosts in Identity Stores	8-23
Deleting Internal Hosts	8-25
Viewing and Performing Bulk Operations for Internal Identity Store Hosts	8-25
Management Hierarchy	8-26
Managing External Identity Stores	8-29
LDAP Overview	8-29
Leveraging Cisco NAC Profiler as an External MAB Database	8-45
Microsoft AD	8-52
RSA SecurID Server	8-80
RADIUS Identity Stores	8-86
Configuring CA Certificates	8-95
Adding a Certificate Authority	8-95
Editing a Certificate Authority and Configuring Certificate Revocation Lists	8-96
Deleting a Certificate Authority	8-98
Exporting a Certificate Authority	8-99

Configuring Certificate Authentication Profiles	8-99
Configuring Identity Store Sequences	8-101
Creating, Duplicating, and Editing Identity Store Sequences	8-102
Deleting Identity Store Sequences	8-104

CHAPTER 9

Managing Policy Elements 9-1

Managing Policy Conditions	9-1
Creating, Duplicating, and Editing a Date and Time Condition	9-3
Creating, Duplicating, and Editing a Custom Session Condition	9-5
Deleting a Session Condition	9-6
Managing Authorizations and Permissions	9-17
Creating, Duplicating, and Editing Authorization Profiles for Network Access	9-18
Creating and Editing Security Groups	9-22
Creating, Duplicating, and Editing a Shell Profile for Device Administration	9-23
Creating, Duplicating, and Editing Command Sets for Device Administration	9-28
Creating, Duplicating, and Editing Downloadable ACLs	9-30
Deleting an Authorizations and Permissions Policy Element	9-32
Configuring Security Group Access Control Lists	9-32

CHAPTER 10

Managing Access Policies 10-1

Policy Creation Flow	10-1
Network Definition and Policy Goals	10-2
Policy Elements in the Policy Creation Flow	10-2
Access Service Policy Creation	10-4
Service Selection Policy Creation	10-4
Customizing a Policy	10-4
Configuring the Service Selection Policy	10-5
Configuring a Simple Service Selection Policy	10-6
Service Selection Policy Page	10-6
Creating, Duplicating, and Editing Service Selection Rules	10-8
Displaying Hit Counts	10-10
Deleting Service Selection Rules	10-10
Configuring Access Services	10-11
Editing Default Access Services	10-11
Creating, Duplicating, and Editing Access Services	10-12
Deleting an Access Service	10-22
Configuring Access Service Policies	10-23
Viewing Identity Policies	10-23
Configuring Identity Policy Rule Properties	10-26

Configuring a Group Mapping Policy	10-28
Configuring Group Mapping Policy Rule Properties	10-30
Configuring a Session Authorization Policy for Network Access	10-31
Configuring Network Access Authorization Rule Properties	10-33
Configuring Device Administration Authorization Policies	10-33
Configuring Device Administration Authorization Rule Properties	10-34
Configuring Device Administration Authorization Exception Policies	10-35
Configuring Shell/Command Authorization Policies for Device Administration	10-36
Configuring Authorization Exception Policies	10-37
Creating Policy Rules	10-39
Duplicating a Rule	10-40
Editing Policy Rules	10-40
Deleting Policy Rules	10-41
Configuring Compound Conditions	10-41
Compound Condition Building Blocks	10-42
Types of Compound Conditions	10-43
Using the Compound Expression Builder	10-46
Security Group Access Control Pages	10-47
Egress Policy Matrix Page	10-47
Editing a Cell in the Egress Policy Matrix	10-48
Defining a Default Policy for Egress Policy Page	10-48
NDAC Policy Page	10-49
NDAC Policy Properties Page	10-50
Network Device Access EAP-FAST Settings Page	10-51
Maximum User Sessions	10-52
Maximum Session User Settings	10-52
Maximum Session Group Settings	10-53
Maximum Session Global Settings	10-55
Purging User Sessions	10-55
Maximum User Session in Distributed Environment	10-56
Maximum User Session in Proxy Scenario	10-57
Maximum Login Failed Attempts Policy	10-57
Configuring Maximum Login Failed Attempts Count for Users	10-58
Configuring Maximum Login Failed Attempts Count for Identity Groups	10-59
Configuring Maximum Login Failed Attempts Count for Users Globally	10-59

CHAPTER 11
Monitoring and Reporting in ACS 11-1

Authentication Records and Details	11-2
Dashboard Pages	11-2

Working with Portlets	11-4
Working with the Authentication Lookup Portlet	11-5
Configuring Tabs in the Dashboard	11-6
Adding Tabs to the Dashboard	11-6
Renaming Tabs in the Dashboard	11-7
Changing the Dashboard Layout	11-8
Deleting Tabs from the Dashboard	11-8

CHAPTER 12

Managing Alarms	12-1
Understanding Alarms	12-1
Evaluating Alarm Thresholds	12-2
Notifying Users of Events	12-2
Viewing and Editing Alarms in Your Inbox	12-3
Understanding Alarm Schedules	12-8
Creating and Editing Alarm Schedules	12-9
Assigning Alarm Schedules to Thresholds	12-10
Deleting Alarm Schedules	12-10
Creating, Editing, and Duplicating Alarm Thresholds	12-11
Configuring General Threshold Information	12-16
Configuring Threshold Criteria	12-16
Configuring Threshold Notifications	12-35
Deleting Alarm Thresholds	12-36
Configuring System Alarm Settings	12-37
Understanding Alarm Syslog Targets	12-38
Creating and Editing Alarm Syslog Targets	12-38
Deleting Alarm Syslog Targets	12-39

CHAPTER 13

Managing Reports	13-1
ACS Reports	13-2
Running Reports	13-3
Reports Navigation	13-3
Show or Hide Columns in Reports Table	13-5
Fixing Columns in Reports Table	13-6
Sorting Data in Reports Table	13-7
Filtering Data in Reports Table	13-7
Exporting Reports	13-8
Saving and Scheduling Reports	13-9
Saved Reports	13-9

Scheduled Reports	13-11
Favorite Reports	13-14
Adding Favorite Reports	13-14
Deleting Reports from Favorites	13-14
Available Reports	13-15
Available Filters	13-20
Changing Authorization for RADIUS Active Sessions Dynamically	13-22
Enabling RADIUS CoA Options on a Device	13-23
Changing Authorization and Disconnecting Active RADIUS Sessions	13-24
Understanding Charts	13-25

CHAPTER 14
Troubleshooting ACS with the Monitoring and Report Viewer 14-1

Available Diagnostic and Troubleshooting Tools	14-1
Connectivity Tests	14-1
ACS Support Bundle	14-1
Expert Troubleshooter	14-2
Performing Connectivity Tests	14-3
Downloading ACS Support Bundles for Diagnostic Information	14-4
Working with Expert Troubleshooter	14-5
Troubleshooting RADIUS Authentications	14-6
Executing the Show Command on a Network Device	14-9
Evaluating the Configuration of a Network Device	14-10
Comparing SGACL Policy Between a Network Device and ACS	14-11
Comparing the SXP-IP Mappings Between a Device and its Peers	14-12
Comparing IP-SGT Pairs on a Device with ACS-Assigned SGT Records	14-14
Comparing Device SGT with ACS-Assigned Device SGT	14-15

CHAPTER 15
Managing System Operations and Configuration in the Monitoring and Report Viewer 15-1

Configuring Data Purging and Incremental Backup	15-3
Configuring NFS Staging	15-7
Restoring Data from a Backup	15-7
Viewing Log Collections	15-8
Log Collection Details Page	15-9
Recovering Log Messages	15-12
Viewing Scheduled Jobs	15-12
Viewing Process Status	15-13
Viewing Data Upgrade Status	15-14

Viewing Failure Reasons	15-15
Editing Failure Reasons	15-15
Specifying E Mail Settings	15-16
SNMP Traps	15-16
Configuring SNMP Server to Receive Traps from ACS	15-17
SNMP Traps for Monitoring Disk Utilization	15-17
Configuring SNMP Preferences	15-19
Understanding Collection Filters	15-19
Creating and Editing Collection Filters	15-20
Deleting Collection Filters	15-20
Configuring System Alarm Settings	15-21
Configuring Alarm Syslog Targets	15-21
Configuring Remote Database Settings	15-21
Changing the Port Numbers for Oracle Database	15-23

CHAPTER 16

Managing System Administrators	16-1
Understanding Administrator Roles and Accounts	16-2
Understanding Authentication	16-3
Configuring System Administrators and Accounts	16-3
Understanding Roles	16-3
Permissions	16-4
Predefined Roles	16-5
Changing Role Associations	16-7
Administrator Accounts and Role Association	16-7
Creating, Duplicating, Editing, and Deleting Administrator Accounts	16-8
Exporting Administrator Accounts	16-11
Enable and Disable Password Hashing for Internal Administrators	16-12
Viewing Predefined Roles	16-13
Viewing Role Properties	16-14
Configuring Authentication Settings for Administrators	16-14
Configuring Session Idle Timeout	16-17
Configuring Administrator Access Settings	16-17
Working with Administrative Access Control	16-18
Administrator Identity Policy	16-19
Configuring Identity Policy Rule Properties	16-22
Authenticating Administrators against RADIUS Identity and RSA SecurID Servers	16-23
Authenticating Administrators against RADIUS Identity Server	16-24

Authenticating Administrators against RSA SecurID Server	16-24
Administrator Authorization Policy	16-26
Configuring Administrator Authorization Policies	16-27
Configuring Administrator Authorization Rule Properties	16-28
Administrator Login Process	16-29
Resetting the Administrator Password	16-29
Changing the Administrator Password	16-30
Changing Your Own Administrator Password	16-30
Resetting Another Administrator's Password	16-30

CHAPTER 17

Configuring System Operations	17-1
Understanding Distributed Deployment	17-2
Activating Secondary Servers	17-3
Removing Secondary Servers	17-4
Promoting a Secondary Server	17-4
Understanding Local Mode	17-4
Understanding Full Replication	17-5
Specifying a Hardware Replacement	17-6
Scheduled Backups	17-6
Creating, Duplicating, and Editing Scheduled Backups	17-7
Backing Up Primary and Secondary Instances	17-8
Synchronizing Primary and Secondary Instances After Backup and Restore	17-9
Editing Instances	17-10
Viewing and Editing a Primary Instance	17-10
Viewing and Editing a Secondary Instance	17-14
Deleting a Secondary Instance	17-15
Activating a Secondary Instance	17-15
Registering a Secondary Instance to a Primary Instance	17-16
Deregistering Secondary Instances from the Distributed System Management Page	17-19
Deregistering a Secondary Instance from the Deployment Operations Page	17-19
Promoting a Secondary Instance from the Distributed System Management Page	17-20
Promoting a Secondary Instance from the Deployment Operations Page	17-21
Replicating a Secondary Instance from a Primary Instance	17-21
Replicating a Secondary Instance from the Distributed System Management Page	17-21
Replicating a Secondary Instance from the Deployment Operations Page	17-22
Changing the IP address of a Primary Instance from the Primary Server	17-23
Failover	17-23
Using the Deployment Operations Page to Create a Local Mode Instance	17-24

Creating, Duplicating, Editing, and Deleting Software Repositories	17-25
Managing Software Repositories from the Web Interface and CLI	17-26
Configuring RSA Public Key for Authentication against SFTP Repositories	17-27
Exporting Policies from ACS Web Interface	17-30
Trust Communication in a Distributed Deployment	17-31
Configuring Trust Communication in a Distributed Deployment	17-32

CHAPTER 18

Managing System Administration Configurations	18-1
Configuring Global System Options	18-1
Configuring TACACS+ Settings	18-1
Configuring EAP-TLS Settings	18-2
Configuring PEAP Settings	18-3
Configuring HTTP Proxy Settings for CRL Requests	18-3
Configuring EAP-FAST Settings	18-4
Generating EAP-FAST PAC	18-4
Configuring RSA SecurID Prompts	18-5
Managing Dictionaries	18-6
Viewing RADIUS and TACACS+ Attributes	18-6
Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes	18-7
Creating, Duplicating, and Editing RADIUS Vendor-Specific Subattributes	18-10
Viewing RADIUS Vendor-Specific Subattributes	18-11
Configuring Identity Dictionaries	18-12
Creating, Duplicating, and Editing an Internal User Identity Attribute	18-12
Configuring Internal Identity Attributes	18-13
Deleting an Internal User Identity Attribute	18-14
Creating, Duplicating, and Editing an Internal Host Identity Attribute	18-14
Deleting an Internal Host Identity Attribute	18-15
Adding Static IP address to Users in Internal Identity Store	18-15
Configuring Local Server Certificates	18-16
Adding Local Server Certificates	18-16
Importing Server Certificates and Associating Certificates to Protocols	18-17
Generating Self-Signed Certificates	18-18
Generating a Certificate Signing Request	18-19
Binding CA Signed Certificates	18-20
Editing and Renewing Certificates	18-20
Exporting Certificates	18-22
Viewing Outstanding Signing Requests	18-22
Configuring Local and Remote Log Storage	18-23
Configuring Remote Log Targets	18-23

Deleting a Remote Log Target	18-26
Configuring the Local Log	18-27
Deleting Local Log Data	18-27
Configuring Logging Categories	18-28
Displaying Logging Categories	18-35
Configuring the Log Collector	18-36
Viewing the Log Message Catalog	18-36
Exporting Messages from the Log Message Catalog	18-37
Licensing Overview	18-37
Types of Licenses	18-38
Installing a License File	18-39
Viewing and Upgrading the Base Server License	18-39
Viewing License Feature Options	18-41
Adding Deployment License Files	18-42
Deleting Deployment License Files	18-43
Available Downloads	18-43
Downloading Migration Utility Files	18-44
Downloading UCP Web Service Files	18-44
Downloading Sample Python Scripts	18-44
Downloading Rest Services	18-45

APPENDIX A
Understanding Logging A-1

About Logging	A-1
Using Log Targets	A-2
Logging Categories	A-2
Global and Per-Instance Logging Categories	A-4
Log Message Severity Levels	A-4
Local Store Target	A-5
Remote Syslog Server Target	A-8
Monitoring and Reports Server Target	A-10
Viewing Log Messages	A-10
Debug Logs	A-11
ACS 4.x Versus ACS 5.8.1 Logging	A-11

APPENDIX B
AAA Protocols B-1

Typical Use Cases	B-1
Device Administration (TACACS+)	B-1
Network Access (RADIUS With and Without EAP)	B-2

Access Protocols—TACACS+ and RADIUS	B-5
Overview of TACACS+	B-5
Overview of RADIUS	B-6
RADIUS IETF	B-6
RADIUS VSAs	B-6
ACS 5.8.1 as the AAA Server	B-7
RADIUS Attribute Support in ACS 5.8.1	B-8
RADIUS Access Requests	B-10

APPENDIX C

Authentication in ACS 5.8.1	C-1
Authentication Considerations	C-1
Authentication and User Databases	C-1
PAP	C-2
RADIUS PAP Authentication	C-3
EAP	C-3
EAP-MD5	C-5
Overview of EAP-MD5	C-5
EAP- MD5 Flow in ACS 5.8.1	C-5
EAP-TLS	C-5
Overview of EAP-TLS	C-6
PKI Credentials	C-8
Acquiring Local Certificates	C-9
Exporting Credentials	C-11
Credentials Distribution	C-12
Securing the Cryptographic Sensitive Material	C-12
EAP-TLS Flow in ACS 5.8.1	C-13
PEAPv0/1	C-14
Overview of PEAP	C-15
PEAP Flow in ACS 5.8.1	C-17
EAP-FAST	C-19
Overview of EAP-FAST	C-19
EAP-FAST in ACS 5.8.1	C-21
EAP-FAST Flow in ACS 5.8.1.	C-27
EAP-FAST PAC Management	C-28
EAP Authentication with RADIUS Key Wrap	C-30
EAP-MSCHAPv2	C-30
Overview of EAP-MSCHAPv2	C-30
EAP- MSCHAPv2 Flow in ACS 5.8.1	C-31

CHAP	C-32
LEAP	C-32
Certificate Attributes	C-32
Certificate Binary Comparison	C-33
Certificate Revocation	C-34
Machine Authentication	C-35
Authentication Protocol and Identity Store Compatibility	C-36

APPENDIX D

Open Source License Acknowledgments	D-1
Notices	D-1
OpenSSL/Open SSL Project	D-1



Preface

Revised: July 25, 2017

This guide describes how to use Cisco Secure Access Control System (ACS) 5.8.1.

Audience

This guide is for security administrators who use ACS, and who set up and maintain network and application security.

Document Conventions

This guide uses the convention whereby the symbol ^ represents the key labeled *Control*. For example, the key combination ^z means hold down the **Control** key while you press the **z** key.

Command descriptions use these conventions:

- Examples that contain system prompts denote interactive sessions, indicating the commands that you should enter at the prompt. The system prompt indicates the current level of the EXEC command interpreter. For example, the prompt `Router>` indicates that you should be at the *user* level, and the prompt `Router#` indicates that you should be at the *privileged* level. Access to the privileged level usually requires a password.
- Commands and keywords are in **boldface** font.
- Arguments for which you supply values are in *italic* font.
- Elements in square brackets ([]) are optional.
- Alternative keywords of which you must choose one are grouped in braces ({ }) and separated by vertical bars (|).

Examples use these conventions:

- Terminal sessions and sample console screen displays are in `screen` font.
- Information you enter is in **boldface screen** font.
- Nonprinting characters, such as passwords, are in angle brackets (< >).
- Default responses to system prompts are in square brackets ([]).
- An exclamation point (!) at the beginning of a line indicates a comment line.



Caution

Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.



Note

Means *the described action saves time*. You can save time by performing the action described in the paragraph.



Note

Means *reader take note*. Notes identify important information that you should reflect upon before continuing, contain helpful suggestions, or provide references to materials not contained in the document.

Documentation Updates

[Table 1](#) lists the updates to the *User Guide for Cisco Secure Access Control System 5.8.1*.

Table 1 *Updates to the User Guide for Cisco Secure Access Control System 5.8.1*

Date	Description
03/21/2016	Cisco Secure Access Control System, Release 5.8.1.

Related Documentation

[Table 2](#) lists a set of related technical documentation available on Cisco.com. To find end-user documentation for all products on Cisco.com, go to: <http://www.cisco.com/go/techdocs>.

Select **Products > Security > Access Control and Policy > Cisco Secure Access Control System > Cisco Secure Access Control System 5.8.1**.



Note

It is possible for the printed and electronic documentation to be updated after original publication. Therefore, you should also review the documentation on <http://www.cisco.com> for any updates.

Table 2 *Product Documentation*

Document Title	Available Formats
<i>Cisco Secure Access Control System In-Box Documentation and China RoHS Pointer Card</i>	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-documentation-roadmaps-list.html
<i>Migration Guide for Cisco Secure Access Control System 5.8.1</i>	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-installation-guides-list.html
<i>CLI Reference Guide for Cisco Secure Access Control System 5.8.1</i>	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-command-reference-list.html

Table 2 *Product Documentation (continued)*

Document Title	Available Formats
<i>Supported and Interoperable Devices and Software for Cisco Secure Access Control System 5.8.1</i>	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-device-support-tables-list.html
Installation and Upgrade Guide for Cisco Secure Access Control System 5.8.1	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-installation-guides-list.html
<i>Release Notes for Cisco Secure Access Control System 5.8.1</i>	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-release-notes-list.html
Software Developer's Guide for Cisco Secure Access Control System 5.8.1	http://www.cisco.com/c/en/us/support/security/secure-access-control-system/products-programming-reference-guides-list.html
<i>Regulatory Compliance and Safety Information for Cisco Secure Access Control System</i>	http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-6/regulatory/compliance/csacsrcsi.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.





Introducing ACS 5.8.1

This section contains the following topics:

- [Overview of ACS, page 1-1](#)
- [ACS Distributed Deployment, page 1-2](#)
- [ACS Management Interfaces, page 1-3](#)

Overview of ACS

ACS is a policy-based security server that provides standards-compliant Authentication, Authorization, and Accounting (AAA) services to your network. ACS facilitates the administrative management of Cisco and non-Cisco devices and applications.

As a dominant enterprise network access control platform, ACS serves as an integration point for network access control and identity management.

ACS 5.x provides a rule-based policy model that allows you to control network access based on dynamic conditions and attributes. The rule-based policy is designed to meet complex access policy needs. For more information on the rule-based policy model in ACS, see [ACS 5.x Policy Model, page 3-1](#)

Within the greater context of two major AAA protocols—RADIUS and TACACS+—ACS provides the following basic areas of functionality:

- Under the framework of the RADIUS protocol, ACS controls the wired and wireless access by users and host machines to the network and manages the accounting of the network resources used.

ACS supports multiple RADIUS-based authentication methods that includes PAP, CHAP, MSCHAPv1, MSCHAPv2. It also supports many members of the EAP family of protocols, such as EAP-MD5, LEAP, PEAP, EAP-FAST, and EAP-TLS.

In association with PEAP or EAP-FAST, ACS also supports EAP-MSCHAPv2, EAP-GTC, and EAP-TLS. For more information on authentication methods, see [Authentication in ACS 5.8.1](#).

- Under the framework of the TACACS+ protocol, ACS helps to manage Cisco and non-Cisco network devices such as switches, wireless access points, routers, and gateways. It also helps to manage services and entities such as dialup, Virtual Private Network (VPN), and firewall.

ACS is the point in your network that identifies users and devices that try to connect to your network. This identity establishment can occur directly by using the ACS internal identity repository for local user authentication or by using external identity repositories.

For example, ACS can use Active Directory as an external identity repository, to authenticate a user to grant the user access to the network. For more information about creating identities and supported identity services, see [Managing Users and Identity Stores, page 8-1](#)

ACS provides advanced monitoring, reporting, and troubleshooting tools that help you administer and manage your ACS deployments. For more information on the monitoring, reporting, and troubleshooting capabilities of ACS, see [Monitoring and Reporting in ACS, page 11-1](#).

For more information about using ACS for device administration and network access scenarios, see [Common Scenarios Using ACS, page 4-1](#)

Cisco Secure ACS:

- Enforces access policies for VPN and wireless users.
- Provides simplified device administration.
- Provides advanced monitoring, reporting, and troubleshooting tools.

There are several changes and enhancements in ACS 5.8.1 compared to ACS 5.7. For a complete list of new and changed features, see [Release Notes for Cisco Secure Access Control System 5.8.1](#).

Related Topics

- [ACS Distributed Deployment, page 1-2](#)
- [ACS Management Interfaces, page 1-3](#)

ACS Distributed Deployment

ACS 5.8.1 is delivered preinstalled on a standard Cisco Linux-based appliance, and supports a fully distributed deployment.

An ACS deployment can consist of a single instance, or multiple instances deployed in a distributed manner, where all instances in a system are managed centrally. One ACS instance becomes the *primary instance* and you can register additional ACS instances to the primary instance as *secondary instances*. All instances have the configuration for the entire deployment, which provides redundancy for configuration data.

The primary instance centralizes the configuration of the instances in the deployment. Configuration changes made in the primary instance are automatically replicated to the secondary instance.

You can force a *full replication* to the secondary instance. Full replication is used when a new secondary instance is registered and in other cases when the replication gap between the secondary instance and the primary instance is significant.

Related Topic

- [ACS 4.x and 5.8.1 Replication, page 1-2](#)

ACS 4.x and 5.8.1 Replication

In ACS 4.x, you must select the database object types (or classes) you wish to replicate from primary instance to the secondary instance. When you replicate an object, a complete configuration copy is made on the secondary instance.

In ACS 5.8.1, any configuration changes made in the primary instance are immediately replicated to the secondary instance. Only the configuration changes made *since the last replication* are propagated to the secondary instance.

ACS 4.x did not provide incremental replication, only full replication, and there was service downtime for replication. ACS 5.8.1 provides incremental replications with no service downtime.

You can also *force* a full replication to the secondary instance if configuration changes do not replicate it. Full replication is used when a new secondary instance is registered and other cases when the replication gap between the secondary instance and the primary instance is significant.

[Table 1-1](#) lists some of the differences between ACS 4.x and 5.8.1 replication.

Table 1-1 *Differences Between ACS 4.x and 5.8.1 Replication*

ACS 4.x	ACS 5.8.1
You can choose the data items to be replicated.	You cannot choose the data items to be replicated. All data items, by default are replicated.
Supports multi-level or cascading replication.	Supports only a fixed flat replication. Cascading replication is not supported.
Some data items, such as the external database configurations, are not replicated.	All data items are replicated except the database key, database certificate, and master keys. The server certificates, Certificate Signing Requests (CSRs), and private keys are replicated, but they are not shown in the interface.

For more information about setting up a distributed deployment, see [Chapter 17, “Configuring System Operations”](#).



Note

Replication does not work in ACS servers if you use the Cisco Overlay Transport Virtualization technology in your Virtual Local Area Network.



Note

Network Address Translation (NAT) is not supported in an ACS distributed deployment environment. That is, if the network address of a primary or secondary instance is translated, then the database replication may not work properly, and it may display a shared secret mismatch error.

ACS Licensing Model

You must have a valid license to operate ACS; ACS prompts you to install a valid base license when you first access the web interface. Each server requires a unique base license in a distributed deployment.

For information about the types of licenses you can install, see [Types of Licenses, page 18-38](#). For more information about licenses, see [Licensing Overview, page 18-37](#).

Related Topic

- [ACS Distributed Deployment, page 1-2](#)

ACS Management Interfaces

This section contains the following topics:

- [ACS Web-Based Interface, page 1-4](#)
- [ACS Command-Line Interface, page 1-4](#)
- [ACS Programmatic Interfaces, page 1-5](#)

ACS Web-Based Interface

You can use the ACS web-based interface to fully configure your ACS deployment, and perform monitoring and reporting operations. The web interface provides a consistent user experience, regardless of the particular area that you are configuring.

The ACS web interface is supported on HTTPS-enabled Microsoft Internet Explorer and Mozilla Firefox browsers. For more information on supported browser versions, see [Release Notes for Cisco Secure Access Control System 5.8.1](#).

The new web interface design and organization:

- Reflects the new policy model, which is organized around the user's view of policy administration. The new policy model is easier to use, as it separates the complex interrelationships that previously existed among policy elements.

For example, user groups, network device groups (NDGs), network access filters, network access profiles, and so on.

- Presents the configuration tasks in a logical order that you can follow for many common scenarios. For example, first you configure conditions and authorizations for policies in the Policy Elements drawer, and then you move on to the Policies drawer to configure the policies with the defined policy elements.
- Provides new page functionality, such as sorting and filtering lists of items.

See [Using the Web Interface, page 5-4](#) for more information.



Note

ACS does not support forward, back, and refresh options that are available on the browser. The ACS web interface does not return any data when you click any of the three options. You need to log out and login again to start working on ACS.



Note

ACS web interface does not support few special characters which you cannot manually enter in the web interface. Therefore, it is not recommended to copy and paste the special characters that are not supported by ACS web interface for certain fields.

Related Topics

- [ACS Command-Line Interface, page 1-4](#)

ACS Command-Line Interface

You can use the ACS command-line interface (CLI), a text-based interface, to perform some configuration and operational tasks and monitoring. Access to the ACS-specific CLI requires administrator authentication by ACS 5.8.1.

You do not need to be an ACS administrator or log in to ACS 5.8.1 to use the non-ACS configuration mode. ACS configuration mode command sessions are logged to the diagnostics logs.

ACS 5.8.1 is shipped on the Cisco SNS-3595 or SNS-3515 appliance.

The ADE-OS software supports the following command modes:

- EXEC—Use EXEC mode commands to perform system-level operation tasks. For example, install, start, and stop an application; copy files and installations; restore backups; and display information.

In addition, certain EXEC mode commands have ACS-specific abilities. For example, start an ACS instance (`acs start`), display and export ACS logs, and reset an ACS configuration to factory default settings (`application reset-config acs`). Such commands are specifically mentioned in the documentation.

- **ACS configuration**—Use these commands to set the debug log level (enable or disable) for the ACS management and runtime components and to show system settings.
- **Configuration**—Use these commands to perform additional configuration tasks for the appliance server in an ADE-OS environment.

**Note**

The CLI includes an option to reset the configuration, which, when issued, resets all ACS configuration information, but retains the appliance settings such as network configuration.

For information about using the CLI, see the *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.8.1*.

Related Topic

- [ACS Web-Based Interface, page 1-4](#)

ACS Programmatic Interfaces

ACS 5.8.1 provides web services and command-line interface (CLI) commands that allow software developers and system integrators to programmatically access some ACS features and functions. ACS 5.8.1 also provides access to the Monitoring and Report Viewer database and web services that allow you to create custom applications to monitor and troubleshoot events in ACS.

The UCP web service allows users, defined in the ACS internal database, to first authenticate and then change their own password. ACS exposes the UCP web service to allow you to create custom web-based applications that you can deploy in your enterprise.

You can develop shell scripts using the CLI commands that ACS offers to perform (CRUD) create, read, update, and delete operations on ACS objects. You can also create an automated shell script to perform bulk operations.

The REST PI (Representational State Transfer Programming Interface) allows you to manage entities such as users, hosts, identity groups, network devices, network device groups, network device group types, and maximum user and group session settings on your own management applications and move these entities into ACS. This way you can define these entities and then use them on your own systems and on ACS.

For more information on how to access these web services and their functionalities, see the [Software Developer's Guide for Cisco Secure Access Control System](#).

Hardware Models Supported by ACS

Table 1-2 displays the details of the hardware models supported by ACS 5.8.1.

Table 1-2 *Hardware Models Supported by ACS 5.8.1*

Hardware Appliance	HDD	RAM	Core	NIC
UCS (SNS-3595)	4 x 600 GB	64 GB	8 cores	2 x 2 (6-1 Gb)
UCS (SNS-3515)	600 GB	16 GB	6 cores	2 x 2 (6-1 Gb)
UCS (SNS-3495)	2 x 600 GB	32 GB	8 cores	2 x 2 (4-1 Gb)
UCS (SNS-3415)	600 GB	16 GB	4 cores	2 x 2 (4-1 Gb)
IBM 1121	2 x 250 GB	4 GB	—	4X10,100,1000 RJ-45
VMWare ESX i5.5 and i6.0	60 to 750 GB	4 to 64 GB	—	2 NICs



Note

Cisco recommends you to use more than a 4GB RAM platform for a deployment that has more than 100,000 devices. ACS runtime crashes when you use a machine with 4GB RAM or less in a deployment that has more than 100,000 devices.



Migrating from ACS 4.x to ACS 5.8.1

ACS 4.x stores policy and authentication information, such as TACACS+ command sets, in the user and user group records. In ACS 5.8.1, policy and authentication information are independent shared components that you use as building blocks when you configure policies.

The most efficient way to make optimal use of the new policy model is to rebuild policies by using the building blocks, or policy elements, of the new policy model. This method entails creating appropriate identity groups, network device groups (NDGs), conditions, authorization profiles, and rules.

ACS 5.8.1 provides a migration utility to transfer data from migration-supported versions of ACS 4.x to an ACS 5.8.1 machine. The ACS 5.8.1 migration process requires, in some cases, administrative intervention to manually resolve data before you import it to ACS 5.8.1.

This process is different from the process of upgrading from versions of ACS 3.x to ACS 4.x, where the ACS 4.x system works the same way as ACS 3.x and no administrative intervention is required.

The migration utility in ACS 5.8.1 supports multiple-instance migration that migrates all ACS 4.x servers in your deployment to ACS 5.8.1. For more information on multiple-instance migration, see the [Migration Guide for Cisco Secure Access Control System 5.8.1](#).

Upgrade refers to the process of transferring data from ACS 5.5 or 5.7 servers to ACS 5.8.1. For information on the upgrade process, see the [Installation and Upgrade Guide for Cisco Secure Access Control System 5.8.1](#).

This chapter contains the following sections:

- [Overview of the Migration Process, page 2-1](#)
- [Before You Begin, page 2-2](#)
- [Downloading Migration Files, page 2-3](#)
- [Migrating from ACS 4.x to ACS 5.8.1, page 2-3](#)
- [Functionality Mapping from ACS 4.x to ACS 5.8.1, page 2-4](#)
- [Common Scenarios in Migration, page 2-7](#)

Overview of the Migration Process

The Migration utility completes the data migration process in two phases:

- Analysis and Export
- Import

In the Analysis and Export phase, you identify the objects that you want to export into 5.8.1. The Migration utility analyses the objects, consolidates the data, and exports it.

After the Analysis and Export phase is complete, the Migration utility generates a report that lists any data compatibility errors, which you can manually resolve to successfully import these objects into 5.8.1.

The Analysis and Export phase is an iterative process that you can rerun many times to ensure that there are no errors in the data to be imported. After you complete the Analysis and Export phase, you can run the import phase to import data into ACS 5.8.1.

This section contains the following topics:

- [Migration Requirements, page 2-2](#)
- [Supported Migration Versions, page 2-2](#)

Migration Requirements

To run the Migration utility, you must deploy the following machines:

- The source ACS 4.x machine—This machine can either be an ACS 4.x solution engine or a ACS for Windows 4.x machine. The source machine must be running a migration-supported version of ACS. See [Supported Migration Versions, page 2-2](#) for more information.
- The migration machine—This machine must be a Windows platform that runs the same version of ACS (including the patch) as the source machine. The migration machine cannot be an ACS production machine or an ACS appliance machine. It has to be a Windows server running ACS for Windows. The migration machine requires 2 GB RAM.
- The target ACS 5.8.1 machine—Back up your ACS 5.8.1 configuration data and ensure that the migration interface is enabled on ACS 5.8.1 before you begin the import process. We recommend that you import data into a fresh ACS 5.8.1 database. To enable the migration interface, from the ACS CLI, enter:

```
acs config-web-interface migration enable
```

Supported Migration Versions

ACS 5.8.1 supports migration from the following ACS 4.x versions:

- ACS 4.1.1.24
- ACS 4.1.4
- ACS 4.2.0.124
- ACS 4.2.1



Note

You must install the latest patch for the supported migration versions listed here. Also, if you have any other version of ACS 4.x installed, you must upgrade to one of the supported versions and install the latest patch for that version before you can migrate to ACS 5.8.1.

Before You Begin

Before you migrate data from ACS 4.x to ACS 5.8.1, ensure that you:

- Check for database corruption issues in the ACS 4.x source machine.
- Have the same ACS versions on the source and migration machines (including the patch).
- Have configured a single IP address on the migration machine.
- Back up the source ACS 4.x data.
- Have full network connectivity between the migration machine and the ACS 5.8.1 server.
- Have enabled the migration interface on the ACS 5.8.1 server.
- Use any ACS administrator account with a superadmin role to run the Migration Utility in ACS 5.8.1.

This release of ACS allows administrators with Super Admin role to run the Migration Utility. In earlier releases, you can run the Migration Utility only with the acsadmin account. This limitation is now removed in Cisco Secure ACS, Release 5.8.1.

You cannot use the remote desktop to connect to the migration machine to run the Migration Utility. You must run the Migration Utility on the migration machine; or, use VNC to connect to the migration machine.

**Note**

The ACS 5.8.1 migration utility is not supported on Windows 2008 64 bit.

Downloading Migration Files

To download migration application files and the migration guide for ACS 5.8.1:

-
- | | |
|---------------|--|
| Step 1 | Choose System Administration > Downloads > Migration Utility .
The Migration from 4.x page appears. |
| Step 2 | Click Migration application files to download the application file that you want to use to run the migration utility. |
| Step 3 | Click Migration Guide to download the <i>Migration Guide for Cisco Secure Access Control System 5.8.1</i> . |
-

Migrating from ACS 4.x to ACS 5.8.1

You can migrate data from any of the migration-supported versions of ACS 4.x to ACS 5.8.1. The migration utility migrates the following ACS 4.x data entities:

- Network Device Groups (NDGs)
- AAA Clients and Network Devices
- Internal Users
- User-Defined Fields (from the Interface Configuration section)
- User Groups
- Shared Shell Command Authorization Sets
- User TACACS+ Shell Exec Attributes (migrated to user attributes)

- Group TACACS+ Shell Exec Attributes (migrated to shell profiles)
- User TACACS+ Command Authorization Sets
- Group TACACS+ Command Authorization Sets
- Shared, Downloadable ACLs
- EAP-FAST Master Keys
- Shared RADIUS Authorization Components (RACs)
- RADIUS VSAs

**Note**

The Migration utility does not migrate public key infrastructure (PKI) configuration data and does not support certificate migration.

To migrate data from ACS 4.x to ACS 5.8.1:

-
- Step 1** Upgrade the ACS 4.x version to a migration-supported version if your ACS 4.x server currently does not run one of the migration-supported versions.
- For a list of migration-supported ACS versions, see [Supported Migration Versions, page 2-2](#).
- Step 2** Install the same migration-supported version of ACS on the migration machine, which is a Windows server.
- Step 3** Back up the ACS 4.x data and restore it on the migration machine.
- Step 4** Place the Migration utility on the migration machine.
- You can get the Migration utility from the Installation and Recovery DVD.
- Step 5** Run the Analyze and Export phase of the Migration utility on the migration machine.
- Step 6** Resolve any issues in the Analyze and Export phase.
- Step 7** Run the Import phase of the Migration utility on the migration machine.
- The import phase imports data into the 5.8.1 server.
-

**Note**

If you have a large internal database, then we recommend that you import the data into a standalone 5.x primary server and not to a server that is connected to several secondary servers. After data migration is complete, you can register the secondary servers to the standalone 5.x primary server.

For detailed information about using the migration utility, see the [Migration Guide for Cisco Secure Access Control System 5.8.1](#).

After you migrate the data, you can reconstruct your policies with the migrated objects.

Functionality Mapping from ACS 4.x to ACS 5.8.1

In ACS 5.8.1, you define authorizations, shell profiles, attributes, and other policy elements as independent, reusable objects, and not as part of the user or group definition.

Table 2-1 describes where you configure identities, network resources, and policy elements in ACS 5.8.1. Use this table to view and modify your migrated data identities. See [ACS 5.x Policy Model, page 3-1](#) for an overview of the ACS 5.8.1 policy model.

Table 2-1 *Functionality Mapping from ACS 4.x to ACS 5.8.1*

To configure...	In ACS 4.x, choose...	In ACS 5.8.1, choose...	Additional information for 5.8.1
Network device groups	Network Configuration page	Network Resources > Network Device Groups See Creating, Duplicating, and Editing Network Device Groups, page 7-2 .	You can use NDGs as conditions in policy rules. ACS 5.8.1 does not support NDG shared password. After migration, member devices contain the NDG shared password information.
Network devices and AAA clients	Network Configuration page	Network Resources > Network Devices and AAA Clients See Network Devices and AAA Clients, page 7-5 .	RADIUS KeyWrap keys (KEK and MACK) are migrated from ACS 4.x to ACS 5.8.1.
User groups	Group Setup page	Users and Identity Stores > Identity Groups See Managing Identity Attributes, page 8-7 .	You can use identity groups as conditions in policy rules.
Internal users	User Setup page	Users and Identity Stores > Internal Identity Stores > Users See Managing Internal Identity Stores, page 8-4 .	ACS 5.8.1 authenticates internal users against the internal identity store only. Migrated users that used an external database for authentication have a default authentication password that they must change on first access.
Internal hosts	Network Access Profiles > Authentication	Users and Identity Stores > Internal Identity Stores > Hosts See Creating Hosts in Identity Stores, page 8-23 .	You can use the internal hosts in identity policies for Host Lookup.
Identity attributes (user-defined fields)	Interface Configuration > User Data Configuration	System Administration > Configuration > Dictionaries > Identity > Internal Users See Managing Dictionaries, page 18-6 .	Defined identity attribute fields appear in the User Properties page. You can use them as conditions in access service policies.

Table 2-1 *Functionality Mapping from ACS 4.x to ACS 5.8.1 (continued)*

To configure...	In ACS 4.x, choose...	In ACS 5.8.1, choose...	Additional information for 5.8.1
Command sets (command authorization sets)	One of the following: <ul style="list-style-type: none"> Shared Profile Components > Command Authorization Set User Setup page Group Setup page 	Policy Elements > Authorization and Permissions > Device Administration > Command Set See Creating, Duplicating, and Editing Command Sets for Device Administration , page 9-28.	You can add command sets as results in authorization policy rules in a device administration access service.
Shell exec parameters	User Setup page	System Administration > Dictionaries > Identity > Internal Users See Managing Dictionaries , page 18-6.	Defined identity attribute fields appear in the User Properties page. You can use them as conditions in access service policies.
Shell profiles (shell exec parameters or shell command authorization sets)	Group Setup page	Policy Elements > Authorization and Permissions > Device Administration > Shell Profile See Creating, Duplicating, and Editing a Shell Profile for Device Administration , page 9-23.	You can add shell profiles as results in authorization policy rules in a device administration access service.
Date and time condition (Time of Day Access) You cannot migrate the date and time conditions. You have to recreate them in ACS 5.8.1.	Group Setup page	Policy Elements > Session Conditions > Date and Time See Creating, Duplicating, and Editing a Date and Time Condition , page 9-3.	You can add date and time conditions to a policy rule in the Service Selection policy or in an authorization policy in an access service.
RADIUS Attributes	One of the following: <ul style="list-style-type: none"> Shared Profile Components > RADIUS Authorization Component User Setup page Group Setup page You cannot migrate the RADIUS attributes from user and group setups. You have to recreate them in ACS 5.8.1.	Policy Elements > Authorization and Permissions > Network Access > Authorization Profile > Common Tasks tab or Policy Elements > Authorization and Permissions > Network Access > Authorization Profile > RADIUS Attributes tab See Creating, Duplicating, and Editing Authorization Profiles for Network Access , page 9-18.	You configure RADIUS attributes as part of a network access authorization profile. You can add authorization profiles as results in an authorization policy in a network access service.

Table 2-1 *Functionality Mapping from ACS 4.x to ACS 5.8.1 (continued)*

To configure...	In ACS 4.x, choose...	In ACS 5.8.1, choose...	Additional information for 5.8.1
Downloadable ACLs	Shared Profile Components	Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs See Creating, Duplicating, and Editing Downloadable ACLs , page 9-30.	You can add downloadable ACLs (DACLS) to a network access authorization profile. After you create the authorization profile, you can add it as a result in an authorization policy in a network access service.
RADIUS VSA	Interface Configuration	System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA. See Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes , page 18-7.	You configure RADIUS VSA attributes as part of a network access authorization profile. You can add authorization profiles as results in an authorization policy in a network access service.

Common Scenarios in Migration

The following are some of the common scenarios that you encounter while migrating to ACS 5.8.1:

- [Migrating from ACS 4.2 on CSACS 1121 to ACS 5.8.1](#), page 2-7
- [Migrating from ACS 3.x to ACS 5.8.1](#), page 2-8
- [Migrating Data from Other AAA Servers to ACS 5.8.1](#), page 2-8

Migrating from ACS 4.2 on CSACS 1121 to ACS 5.8.1

In your deployment, if you have ACS 4.2 on the CSACS 1121 and you would like to migrate to ACS 5.8.1, you must do the following:

-
- | | |
|---------------|--|
| Step 1 | Install Cisco Secure Access Control Server 4.2 for Windows on the migration machine. |
| Step 2 | Back up the ACS 4.2 data on the CSACS 1121. |
| Step 3 | Restore the data in the migration machine. |
| Step 4 | Run the Analysis and Export phase of the Migration utility on the migration machine. |
| Step 5 | Install ACS 5.8.1 on the CSACS 1121. |
| Step 6 | Import the data from the migration machine to the CSACS 1121 that has ACS 5.8.1 installed. |
-

For a detailed description of each of these steps, see the [Migration Guide for Cisco Secure Access Control System 5.8.1](#).

Migrating from ACS 3.x to ACS 5.8.1

If you have ACS 3.x deployed in your environment, you cannot directly migrate to ACS 5.8.1. You must do the following:

-
- Step 1** Upgrade to a migration-supported version of ACS 4.x. See [Supported Migration Versions, page 2-2](#) for a list of supported migration versions.
- Step 2** Check the upgrade paths for ACS 3.x:
- For the ACS Solution Engine, see:
http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.1/installation/guide/solution_engine/upgap.html#wp1120037
 - For ACS for Windows, see:
http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4-2/installation/guide/windows/IGwn42/install.html#wp1102849
- Step 3** Upgrade your ACS 3.x server to a migration-supported version of ACS 4.x.
- After the upgrade, follow the steps that describe migrating from ACS 4.x to ACS 5.8.1. Refer to the *Migration Guide for Cisco Secure Access Control System 5.8.1* for more information.
-

Migrating Data from Other AAA Servers to ACS 5.8.1

ACS 5.8.1 allows you to perform bulk import of various ACS objects through the ACS web interface and the CLI. You can import the following ACS objects:

- Users
- Hosts
- Network Devices
- Identity Groups
- NDGs
- Downloadable ACLs
- Command Sets

ACS allows you to perform bulk import of data with the use of a comma-separated values (.csv) file. You must input data in the .csv file in the format that ACS requires. ACS provides a .csv template for the various objects that you can import to ACS 5.8.1. You can download this template from the web interface.

To migrate data from other AAA servers to ACS 5.8.1:

-
- Step 1** Input data into .csv files.
- For more information on understanding .csv templates, see [Software Developer's Guide for Cisco Secure Access Control System 5.8.1](#).
- Step 2** Set up your ACS 5.8.1 appliance.

Step 3 Perform bulk import of data into ACS 5.8.1.

For more information on performing bulk import of ACS objects, see [Software Developer's Guide for Cisco Secure Access Control System 5.8.1](#).

The data from your other AAA servers is now available in ACS 5.8.1.



ACS 5.x Policy Model

ACS 5.x is a policy-based access control system. The term *policy model* in ACS 5.x refers to the presentation of policy elements, objects, and rules to the policy administrator. ACS 5.x uses a rule-based policy model instead of the group-based model used in the 4.x versions.

This section contains the following topics:

- [Overview of the ACS 5.x Policy Model, page 3-1](#)
- [Access Services, page 3-5](#)
- [Service Selection Policy, page 3-12](#)
- [Authorization Profiles for Network Access, page 3-16](#)
- [Policies and Identity Attributes, page 3-17](#)
- [Policies and Network Device Groups, page 3-17](#)
- [Example of a Rule-Based Policy, page 3-18](#)
- [Flows for Configuring Services and Policies, page 3-19](#)



Note

See [Functionality Mapping from ACS 4.x to ACS 5.8.1, page 2-4](#) for a mapping of ACS 4.x concepts to ACS 5.8.1.

Overview of the ACS 5.x Policy Model

The ACS 5.x rule-based policy model provides more powerful and flexible access control than is possible with the older group-based approach.

In the older group-based model, a *group* defines policy because it contains and ties together three types of information:

- Identity information—This information can be based on membership in AD or LDAP groups or a static assignment for internal ACS users.
- Other restrictions or conditions—Time restrictions, device restrictions, and so on.
- Permissions—VLANs or Cisco IOS privilege levels.

The ACS 5.x policy model is based on *rules* of the form:

If condition then result

For example, we use the information described for the group-based model:

If *identity-condition*, *restriction-condition* then *authorization-profile*

In ACS 5.8.1, you define conditions and results as global, shared objects. You define them once and then reference them when you create rules. ACS 5.8.1 uses the term *policy elements* for these shared objects, and they are the building blocks for creating rules.

[Table 3-1](#) shows how the various policy elements define all the information that the old group contained.

Table 3-1 Information in Policy Elements

Information in ACS 4.x Group	Information in ACS 5.8.1 Policy Element
Identity information	<ul style="list-style-type: none">• AD group membership and attributes• LDAP group membership and attributes• ACS internal identity groups and attributes
Other policy conditions	<ul style="list-style-type: none">• Time and date conditions• Custom conditions
Permissions	Authorization profiles

A *policy* is a set of rules that ACS 5.x uses to evaluate an access request and return a decision. For example, the set of rules in an:

- *Authorization policy* return the authorization decision for a given access request.
- *Identity policy* decide how to authenticate and acquire identity attributes for a given access request.

ACS 5.x organizes the sequence of independent policies (a policy work flow) into an *access service*, which it uses to process an access request. You can create multiple access services to process different kinds of access requests; for example, for device administration or network access. For more information, see [Access Services, page 3-5](#).

You can define simple policies and rule-based policies. Rule-based policies are complex policies that test various conditions. Simple policies apply a single result to all requests without any conditions.

There are various types of policies:

For more information on the different types of policies, see [Types of Policies, page 3-4](#).

For more information about policy model terminology, see [Policy Terminology, page 3-2](#).

Related Topics

- [Policies and Identity Attributes, page 3-17](#)
- [Flows for Configuring Services and Policies, page 3-19](#)

Policy Terminology

[Table 3-2](#) describes the rule-based policy terminology.

Table 3-2 *Rule-Based Policy Terminology*

Term	Description
Access service	<p>Sequential set of policies used to process access requests. ACS 5.x allows you to define multiple access services to support multiple, independent, and isolated sets of policies on a single ACS system.</p> <p>There are two default access services: one for device administration (TACACS+ based access to the device shell or CLI) and one for network access (RADIUS-based access to network connectivity).</p>
Policy element	Global, shared object that defines policy conditions (for example, time and date, or custom conditions based on user-selected attributes) and permissions (for example, authorization profiles). The policy elements are referenced when you create policy rules.
Authorization profile	<p>Basic permissions container for a RADIUS-based network access service, which is where you define all permissions to be granted for a network access request.</p> <p>VLANs, ACLs, URL redirects, session timeout or reauthorization timers, or any other RADIUS attributes to be returned in a response, are defined in the authorization profile.</p>
Shell profile	<p>Basic permissions container for TACACS+ based device administration policy. This is where you define permissions to be granted for a shell access request.</p> <p>IOS privilege level, session timeout, and so on are defined in the shell profile.</p>
Command set	Contains the set of permitted commands for TACACS+ based, per-command authorization.
Policy	Set of rules that are used to reach a specific policy decision. For example, how to authenticate and what authorization to grant. For any policies that have a default rule, a policy is a first-match rules table with a default rule for any request which does not match any user-created rules.
Identity policy	ACS 5.8.1 policy for choosing how to authenticate and acquire identity attributes for a given request. ACS 5.8.1 allows two types of identity policies: a simple, static policy, or a rules-based policy for more complex situations.
Identity group mapping policy	<p>Optional policy for mapping identity information collected from identity stores (for example, group memberships and user attributes) to a single ACS identity group.</p> <p>This can help you normalize identity information and map requests to a single identity group, which is just a tag or an identity classification. The identity group can be used as a condition in authorization policy, if desired.</p>
Authorization policy	ACS 5.8.1 policy for assigning authorization attributes for access requests. Authorization policy selects a single rule and populates the response with the contents of the authorization profiles referenced as the result of the rule.
Exception policy	Special option for authorization policy, which allows you to define separately the set of conditions and authorization results for authorization policy exceptions and waivers. If defined, the exception policy is checked before the main (standard) authorization policy.
Default rule	Catchall rule in ACS 5.8.1 policies. You can edit this rule to specify a default result or authorization action, and it serves as the policy decision in cases where a given request fails to match the conditions specified in any user-created rule.

Simple Policies

You can configure all of your ACS policies as rule-based policies. However, in some cases, you can choose to configure a simple policy, which selects a single result to apply to all requests without conditions.

For example, you can define a rule-based authentication policy with a set of rules for different conditions; or, if you want to use the internal database for all authentications, you can define a simple policy.

[Table 3-3](#) helps you determine whether each policy type can be configured as a simple policy.

- If you create and save a simple policy, and then change to a rule-based policy, the simple policy becomes the default rule of the rule-based policy.
- If you have saved a rule-based policy and then change to a simple policy, ACS automatically uses the default rule as the simple policy.

Related Topic

- [Types of Policies, page 3-4](#)

Rule-Based Policies

Rule-based policies have been introduced to overcome the challenges of identity-based policies. In earlier versions of ACS, although membership in a user group gives members access permissions, it also places certain restrictions on them.

When a user requests access, the user's credentials are authenticated using an identity store, and the user is associated with the appropriate user group. Because authorization is tied to user group, all members of a user group have the same access restrictions and permissions at all times.

With this type of policy (the simple policy), permissions are granted based on a user's association with a particular user group. This is useful if the user's identity is the only dominant condition. However, for users who need different permissions under different conditions, this policy does not work.

In ACS 5.x, you can create rules based on various conditions apart from identity. The user group no longer contains all of the information.

For example, if you want to grant an employee full access while working on campus, and restricted access while working remotely, you can do so using the rule-based policies in ACS 5.8.1.

You can base permissions on various conditions besides identity, and permissions are no longer associated with user groups. You can use session and environment attributes, such as access location, access type, health of the end station, date, time, and so on, to determine the type of access to be granted.

Authorization is now based on a set of rules:

If conditions then apply the respective permissions

With rule-based policies, conditions can consist of any combination of available session attributes, and permissions are defined in authorization profiles. You define these authorization profiles to include VLAN, downloadable ACLs, QoS settings, and RADIUS attributes.

Types of Policies

[Table 3-3](#) describes the types of policies that you can configure in ACS.

The policies are listed in the order of their evaluation; any attributes that a policy retrieves can be used in any policy listed subsequently. The only exception is the Identity group mapping policy, which uses only attributes from identity stores.

Table 3-3 ACS Policy Types

Policy	Can Contain Exception Policy?	Simple ¹ and Rule-Based?	Available Dictionaries for Conditions	Available Result Types	Attributes Retrieved
Service Selection Determines the access service to apply to an incoming request.	No	Yes	All except identity store related	Access Service	—
Identity Determines the identity source for authentication.	No	Yes	All except identity store related	Identity Source, Failure options	Identity Attributes; Identity Group for internal ID stores
Identity Group Mapping Defines mapping attributes and groups from external identity stores to ACS identity groups.	No	Yes	Only identity store dictionaries	Identity Group	Identity Group for external ID stores
Network Access Authorization Determines authorization and permissions for network access.	Yes	Rule-based only	All dictionaries	Authorization Profile, Security Group Access	—
Device Administration Authorization Determines authorization and permissions for device administration.	Yes	Rule-based only	All dictionaries	Shell Profile, Command Set	—

1. A simple policy specifies a single set of results that ACS applies to all requests; it is in effect a one-rule policy.

Access Services

Access services are fundamental constructs in ACS 5.x that allow you to configure access policies for users and devices that connect to the network and for network administrators who administer network devices.

In ACS 5.x, authentication and authorization requests are processed by access services. An access service consists of the following elements:

- **Identity Policy**—Specifies how the user should be authenticated and includes the allowed authentication protocols and the user repository to use for password validation.
- **Group Mapping Policy**—Specifies if the user's ACS identity group should be dynamically established based on user attributes or group membership in external identity stores. The user's identity group can be used as part of their authorization.
- **Authorization Policy**—Specifies the authorization rules for the user.

The access service is an independent set of policies used to process an access request.

The ACS administrator might choose to create multiple access services to allow clean separation and isolation for processing different kinds of access requests. ACS provides two default access services:

- Default Device Admin—Used for TACACS+ based access to device CLI
- Default Network Access—Used for RADIUS-based access to network connectivity

You can use the access services as is, modify them, or delete them as needed. You can also create additional access services.

The TACACS+ protocol separates authentication from authorization; ACS processes TACACS+ authentication and authorization requests separately. [Table 3-4](#) describes additional differences between RADIUS and TACACS+ access services.

Table 3-4 *Differences Between RADIUS and TACACS+ Access Services*

Policy Type	TACACS+	RADIUS
Identity	Optional ¹	Required
Group Mapping	Optional	Optional
Authorization	Optional ¹	Required

1. For TACACS+, you must select either Identity or Authorization.

For TACACS+, all policy types are optional; however, you must choose at least one policy type in a service. If you do not define an identity policy for TACACS+, ACS returns authentication failed for an authentication request.

Similarly, if you do not define an authorization policy and if ACS receives a session or command authorization request, it fails. For both RADIUS and TACACS+ access services, you can modify the service to add policies after creation.



Note

Access services do not contain the service selection policy. Service selection rules are defined independently.

You can maintain and manage multiple access services; for example, for different use cases, networks, regions, or administrative domains. You configure a service selection policy, which is a set of service selection rules to direct each new access request to the appropriate access service.

[Table 3-5](#) describes an example of a set of access services.

Table 3-5 *Access Service List*

Access Service A for Device Administration	Access Service B for Access to 802.1X Agentless Hosts	Access Service C for Access from 802.1X Wired and Wireless Devices
Identity Policy A	Identity Policy B	Identity Policy C
Shell/Command Authorization Policy A	Session Authorization Policy B	Session Authorization Policy C

[Table 3-6](#) describes a service selection policy.

Table 3-6 Service Selection Policy

Rule Name	Condition	Result
DevAdmin	protocol = TACACS+	Access Service A
Agentless	Host Lookup = True	Access Service C
Default	—	Access Service B

If ACS 5.8.1 receives a TACACS+ access request, it applies Access Service A, which authenticates the request according to Identity Policy A. It then applies authorizations and permissions according to the shell/command authorization policy. This service handles all TACACS+ requests.

If ACS 5.8.1 receives a RADIUS request that it determines is a host lookup (for example, the RADIUS service-type attribute is equal to *call-check*), it applies Access Service C, which authenticates according to Identity Policy C. It then applies a session authorization profile according to Session Authorization Policy C. This service handles all host lookup requests (also known as MAC Auth Bypass requests).

Access Service B handles other RADIUS requests. This access service authenticates according to Identity Policy B and applies Session Authorization Policy B. This service handles all RADIUS requests except for host lookups, which are handled by the previous rule.

Access Service Templates

ACS contains predefined access services that you can use as a template when creating a new service. When you choose an access service template, ACS creates an access service that contains a set of policies, each with a customized set of conditions.

You can change the structure of the access service by adding or removing a policy from the service, and you can change the structure of a policy by modifying the set of policy conditions. See [Configuring Access Services Templates, page 10-21](#), for a list of the access service templates and descriptions.

RADIUS and TACACS+ Proxy Services

ACS 5.8.1 can function as a RADIUS, RADIUS proxy or TACACS+ proxy server.

- As a RADIUS proxy server, ACS receives authentication and accounting requests from the NAS and forwards the requests to the external RADIUS server.
- As a TACACS+ proxy server, ACS receives authentication, authorization and accounting requests from the NAS and forwards the requests to the external TACACS+ server.

ACS accepts the results of the requests and returns them to the NAS. You must configure the external RADIUS and TACACS+ servers in ACS for ACS to forward requests to them. You can define the timeout period and the number of connection attempts.

The ACS proxy remote target is a list of remote RADIUS and TACACS+ servers that contain the following parameters:

- IP
- Authentication port
- Accounting port
- Shared secret
- Reply timeout
- Number of retries
- Connection port

- Network timeout

The following information is available in the proxy service:

- Remote RADIUS or TACACS+ servers list
- Accounting proxy local/remote/both
- Strip username prefix/suffix

When a RADIUS proxy server receives a request, it forwards it to the first remote RADIUS or TACACS+ server in the list. If the proxy server does not receive a response within the specified timeout interval and the specified number of retries, it forwards the request to the next RADIUS or TACACS+ server in the list.

When the first response arrives from any of the remote RADIUS or TACACS+ servers in the list, the proxy service processes it. If the response is valid, ACS sends the response back to the NAS.

[Table 3-7](#) lists the differences in RADIUS proxy service between ACS 4.2 and 5.8.1 releases.

Table 3-7 *Differences in RADIUS and TACACS+ Proxy Service Between ACS 4.2 and 5.8.1*

Feature	ACS 5.8.1	ACS 4.2
Configurable timeout (RADIUS)	Yes	No
Configurable retry count (RADIUS)	Yes	No
Network timeout (TACACS+)	Yes	No
Authentication and accounting ports (RADIUS)	Yes	Yes
Connection port (TACACS+)	Yes	No
Proxy cycles detection	Yes (For RADIUS only)	No
Username stripping	Yes	Yes
Accounting proxy (local, remote, or both)	Yes	Yes
Account delay timeout support (RADIUS)	No	No

ACS can simultaneously act as a proxy server to multiple external RADIUS and TACACS+ servers. For ACS to act as a proxy server, you must configure a RADIUS or TACACS+ proxy service in ACS. See [Configuring General Access Service Properties, page 10-13](#) for information on how to configure a RADIUS proxy service.

For more information on proxying RADIUS and TACACS+ requests, see [RADIUS and TACACS+ Proxy Requests, page 4-27](#).

Related Topics

- [Policy Terminology, page 3-2](#)
- [Types of Policies, page 3-4](#)
- [Flows for Configuring Services and Policies, page 3-19](#)

Identity Policy

Two primary mechanisms define the mechanism and source used to authenticate requests:

- Password-based—Authentication is performed against databases after the user enters a username and password. Hosts can bypass this authentication by specifying a MAC address. However, for identity policy authentication, host lookup is also considered to be password-based.
- Certificate-based—A client presents a certificate for authentication of the session. In ACS 5.8.1, certificate-based authentication occurs when the PEAP-TLS or EAP-TLS protocol is selected.

In addition, databases can be used to retrieve attributes for the principal in the request.

The identity source is one result of the identity policy and can be one of the following types:

- Deny Access—Access to the user is denied and no authentication is performed.
- Identity Database—Single identity database. When a single identity database is selected as the result of the identity policy, either an external database (LDAP or AD) or an internal database (users or hosts) is selected as the result.

The database selected is used to authenticate the user/host and to retrieve any defined attributes stored for the user/host in the database.

- Certificate Authentication Profile—Contains information about the structure and content of the certificate, and specifically maps certificate attribute to internal username. For certificate-based authentication, you must select a certificate authentication profile.

For certificate based requests, the entity which identifies itself with a certificate holds the private key that correlates to the public key stored in the certificate. The certificate authentication profile extends the basic PKI processing by defining the following:

- The certificate attribute used to define the username. You can select a subset of the certificate attributes to populate the *username* field for the context of the request. The username is then used to identify the user for the remainder of the request, including the identification used in the logs.
 - The LDAP or AD database to use to verify the revocation status of the certificate. When you select an LDAP or AD database, the certificate data is retrieved from the LDAP or AD database and compared against the data entered by the client in order to provide additional verification of the client certificate.
- Identity Sequence—Sequences of the identity databases. The sequence is used for authentication and, if specified, an additional sequence is used to retrieve only attributes. You can select multiple identity methods as the result of the identity policy. You define the identity methods in an identity sequence object, and the methods included within the sequence may be of any type.

There are two components to an identity sequence: one for authentication, and one for attribute retrieval. The administrator can select to perform authentication based on a certificate or an identity database or both.

- If you choose to perform authentication based on a certificate, ACS selects a single certificate authentication profile.
- If you choose to perform authentication based on an identity database, you must define a list of databases to be accessed in sequence until authentication succeeds. When authentication succeeds, any defined attributes within the database are retrieved.

In addition, you can define an optional list of databases from which additional attributes are retrieved. These additional databases can be accessed irrespective of whether password- or certificate-based authentication was used.

When certificate-based authentication is used, the username field is populated from a certificate attribute and is used to retrieve attributes. All databases defined in the list are accessed and, in cases where a matching record for the user is found, the corresponding attributes, are retrieved.

Attributes can be retrieved for a user even if the user's password is marked that it needs to be changed or if the user account is disabled. Even when you disable a user's account, the user's attributes are still available as a source of attributes, but not for authentication.

Failure Options

If a failure occurs while processing the identity policy, the failure can be one of three main types:

- Authentication failed—ACS received an explicit response that the authentication failed. For example, the wrong username or password was entered, or the user was disabled.
- User/host not found—No such user/host was found in any of the authentication databases.
- Process failed—There was a failure while accessing the defined databases.

All failures returned from an identity database are placed into one of the types above. For each type of failure, you can configure the following options:

- Reject—ACS sends a reject reply.
- Drop—No reply is returned.
- Continue—ACS continues processing to the next defined policy in the service.

The *Authentication Status* system attribute retains the result of the identity policy processing. If you select to continue policy processing in the case of a failure, this attribute can be referred to as a condition in subsequent policy processing to distinguish cases in which identity policy processing did not succeed.

Because of restrictions on the underlying protocol being used, there are cases in which it is not possible to continue processing even if you select the Continue option. This is the case for PEAP, LEAP, and EAP-FAST; even if you select the Continue option, the request is rejected.

The following default values are used for the failure options when you create rules:

- Authentication failed—The default is *reject*.
- User/host not found—The default is *reject*.
- Process failure—The default is *drop*.

Group Mapping Policy

The identity group mapping policy is a standard policy. Conditions can be based on attributes or groups retrieved from the external attribute stores only, or from certificates, and the result is an identity group within the identity group hierarchy.

If the identity policy accesses the internal user or host identity store, then the identity group is set directly from the corresponding user or host record. This processing is an implicit part of the group mapping policy.

Therefore, as part of processing in the group mapping policy, the default rule is only applied if both of the following conditions are true:

- None of the rules in the group mapping table match.
- The identity group is not set from the internal user or host record.

The results of the group mapping policy are stored in the **IdentityGroup** attribute in the System Dictionary and you can include this attribute in policies by selecting the Identity Group condition.

Authorization Policy for Device Administration

Shell profiles determine access to the device CLI; command sets determine TACACS+ per command authorization. The authorization policy for a device administration access service can contain a single shell profile and multiple command sets.

Processing Rules with Multiple Command Sets

It is important to understand how ACS processes the command in the access request when the authorization policy includes rules with multiple command sets. When a rule result contains multiple command sets, and the rule conditions match the access request, ACS processes the command in the access request against each command set in the rule:

-
- | | |
|---------------|--|
| Step 1 | If a command set contains a match for the command and its arguments, and the match has <i>Deny Always</i> , ACS designates the command set as <i>Commandset-DenyAlways</i> . |
| Step 2 | If there is no <i>Deny Always</i> for a command match in a command set, ACS checks all the commands in the command set sequentially for the first match. <ul style="list-style-type: none">• If the first match has <i>Permit</i>, ACS designates the command set as <i>Commandset-Permit</i>.• If the first match has <i>Deny</i>, ACS designates the command set as <i>Commandset-Deny</i>. |
| Step 3 | After ACS has analyzed all the command sets, it authorizes the command: <ul style="list-style-type: none">a. If ACS designated any command set as <i>Commandset-DenyAlways</i>, ACS denies the command.b. If there is no <i>Commandset-DenyAlways</i>, ACS permits the command if any command set is <i>Commandset-Permit</i>; otherwise, ACS denies the command. |
-

Related Topics

- [Policy Terminology, page 3-2](#)
- [Authorization Profiles for Network Access, page 3-16](#)

Exception Authorization Policy Rules

A common real-world problem is that, in day-to-day operations, you often need to grant policy waivers or policy exceptions. A specific user might need special access for a short period of time; or, a user might require some additional user permissions to cover for someone else who is on vacation.

In ACS, you can define an exception policy for an authorization policy. The exception policy contains a separate set of rules for policy exception and waivers, which are typically ad hoc and temporary. The exception rules override the rules in the main rule table.

The exception rules can use a different set of conditions and results from those in the main policy. For example, the main policy might use Identity Group and Location as its conditions, while its related exception policy might use different conditions

By default, exception policies use a compound condition and a time and date condition. The time and date condition is particularly valuable if you want to make sure your exception rules have a definite starting and ending time.

An exception policy takes priority over the main policy. The exception policy does not require its own default rule; if there is no match in the exception policy, the main policy applies, which has its own default rule.

You can use an exception to address a temporary change to a standard policy. For example, if an administrator, *John*, in one group is on vacation, and an administrator, *Bob*, from another group is covering for him, you can create an exception rule that will give *Bob* the same access permissions as *John* for the vacation period.

Related Topics

- [Policy Terminology, page 3-2](#)
- [Policy Conditions, page 3-15](#)
- [Policy Results, page 3-16](#)
- [Policies and Identity Attributes, page 3-17](#)

Service Selection Policy

When ACS receives various access requests, it uses a service selection policy to process the request. ACS provides you two modes of service selection:

- [Simple Service Selection, page 3-12](#)
- [Rules-Based Service Selection, page 3-12](#)

Simple Service Selection

In the simple service selection mode, ACS processes all AAA requests with just one access service and does not actually select a service.

Rules-Based Service Selection

In the rules-based service selection mode, ACS decides which access service to use based on various configurable options. Some of them are:

- AAA Protocol—The protocol used for the request, TACACS+ or RADIUS.
- Request Attributes—RADIUS or TACACS+ attributes in the request.
- Date and Time—The date and time ACS receives the request.
- Network Device Group—The network device group that the AAA client belongs to.
- ACS Server—The ACS server that receives this request.
- AAA Client—The AAA client that sent the request.
- Network condition objects—The network conditions can be based on
 - End Station—End stations that initiate and terminate connections.
 - Device—The AAA client that processes the request.
 - Device Port—In addition to the device, this condition also checks for the port to which the end station is associated with.

For more information on policy conditions, see [Managing Policy Conditions, page 9-1](#).

ACS comes preconfigured with two default access services: Default Device Admin and Default Network Access. The rules-based service selection mode is configured to use the AAA protocol as the selection criterion and hence when a TACACS+ request comes in, the Default Device Admin service is used and when a RADIUS request comes in, the Default Network Access service is used.

Access Services and Service Selection Scenarios

ACS allows an organization to manage its identity and access control requirements for multiple scenarios, such as wired, wireless, remote VPN, and device administration. The access services play a major role in supporting these different scenarios.

Access services allow the creation of distinct and separate network access policies to address the unique policy requirements of different network access scenarios. With distinct policies for different scenarios, you can better manage your organization's network.

For example, the default access services for device administration and network access reflect the typical distinction in policy that is required for network administrators accessing network devices and an organization's staff accessing the company's network.

However, you can create multiple access services to distinguish the different administrative domains. For example, wireless access in the Asia Pacific regions can be administered by a different team than the one that manages wireless access for European users. This situation calls for the following access services:

- APAC-wireless—Access service for wireless users in the Asia Pacific region.
- Europe-wireless—Access service for wireless users in the European countries.

You can create additional access services to reduce complexity in policies within a single access service by creating the complex policy among multiple access services. For example, if a large organization wishes to deploy 802.1x network access, it can have the following access services:

- 802.1x—For machine, user password, and certificate-based authentication for permanent staff.
- Agentless Devices—For devices that do not have an EAP supplicant, such as phones and printers.
- Guest Access—For users accessing guest wireless networks.

In this example, instead of creating the network access policy for 802.1x, agentless devices, and guest access in one access service, the policy is divided into three access services.

First-Match Rule Tables

ACS 5.8.1 provides policy decisions by using first-match rule tables to evaluate a set of rules. Rule tables contain conditions and results. Conditions can be either simple or compound. Simple conditions consist of attribute operator value and are either True or False. Compound conditions contain more complex conditions combined with AND or OR operators. See [Policy Conditions, page 3-15](#) for more information.

The administrator selects simple conditions to be included in a policy. The conditions are displayed as columns in a rule table where the column headings are the condition name, which is usually the name of the attribute.

The rules are displayed under the column headings, and each cell indicates the operator and value that are combined with the attribute to form the condition. If *ANY* [Figure 3-1 on page 14](#) shows a column-based rule table with defined condition types.

Figure 3-1 Example Policy Rule Table

Access Policies > Access Services > Default Device Admin > Authorization

Standard Policy | Exception Policy

Device Administration Authorization Policy

Filter: Status Match if: Equals Clear Filter Go

	<input type="checkbox"/>	Status	Name	Identity Group	NDG: Location	NDG: Device Type	Time And Date	Results	Hit Count
1	<input type="checkbox"/>	●	Sales_Corp_Access	In All Groups: Sales	In All Locations: Boston	-ANY-	match BusHrs	Corp Access	0
2	<input type="checkbox"/>	●	Sales_Guest_Access	In All Groups: Sales	In All Locations: Boston	-ANY-	match NonBusHrs	Guest Access	0
3	<input type="checkbox"/>	●	Engineer_Corp_Access	In All Groups: Engineering	In All Locations: New York	-ANY-	-ANY-	Corp Access	0

** ☐ Default If no rules defined or no enabled rule matches. Permit Access 0

Create... Duplicate... Edit Delete Move to... Customize Hit Count

Save Changes Discard Changes

252961

Table 3-8 Example Policy Rule

Column	Description
Status	<p>You can define the status of a rule as enabled, disabled, or monitored:</p> <ul style="list-style-type: none"> Enabled—ACS evaluates an enabled rule, and when the rule conditions match the access request, ACS applies the rule result. Disabled—The rule appears in the rule table, but ACS skips this rule and does not evaluate it. Monitor Only—ACS evaluates a monitored rule. If the rule conditions match the access request, ACS creates a log record with information relating to the match. <p>ACS does not apply the result, and the processing continues to the following rules. Use this status during a running-in period for a rule to see whether it is needed.</p>
Name	Descriptive name. You can specify any name that describes the rule's purpose. By default, ACS generates rule name strings <i>rule-number</i> .
Conditions	
Identity Group	In this example, this is matching against one of the internal identity groups.
NDG: Location	Location network device group. The two predefined NDGs are Location and Device Type.
Results	

Table 3-8 *Example Policy Rule*

Shell Profile	Used for device administration-type policies and contains permissions for TACACS+ shell access request, such as Cisco IOS privilege level.
Hit Counts	<p>Displays the number of times a rule matched an incoming request since the last reset of the policy's hit counters. ACS counts hits for any monitored or enabled rule whose conditions all matched an incoming request. Hit counts for:</p> <ul style="list-style-type: none"> • Enabled rules reflect the matches that occur when ACS processes requests. • Monitored rules reflect the counts that would result for these rules if they were enabled when ACS processed the requests. <p>The primary server in an ACS deployment displays the hit counts, which represent the total matches for each rule across all servers in the deployment. On a secondary server, all hit counts in policy tables appear as zeroes.</p>

The default rule specifies the policy result that ACS uses when no other rules exist, or when the attribute values in the access request do not match any rules.

ACS evaluates a set of rules in the first-match rule table by comparing the values of the attributes associated with the current access request with a set of conditions expressed in a rule.

- If the attribute values do not match the conditions, ACS proceeds to the next rule in the rule table.
- If the attribute values match the conditions, ACS applies the result that is specified for that rule, and ignores all remaining rules.
- If the attribute values do not match any of the conditions, ACS applies the result that is specified for the policy default rule.

Related Topics

- [Policy Terminology, page 3-2](#)
- [Policy Conditions, page 3-15](#)
- [Policy Results, page 3-16](#)
- [Exception Authorization Policy Rules, page 3-11](#)

Policy Conditions

You can define simple conditions in rule tables based on attributes in:

- Customizable conditions—You can create custom conditions based on protocol dictionaries and identity dictionaries that ACS knows about. You define custom conditions in a policy rule page; you cannot define them as separate condition objects.
- Standard conditions—You can use standard conditions, which are based on attributes that are always available, such as device IP address, protocol, and username-related fields.

Related Topics

- [Policy Terminology, page 3-2](#)
- [Policy Results, page 3-16](#)
- [Exception Authorization Policy Rules, page 3-11](#)
- [Policies and Identity Attributes, page 3-17](#)

Policy Results

Policy rules include result information depending on the type of policy. You define policy results as independent shared objects; they are not related to user or user group definitions.

For example, the policy elements that define authorization and permission results for authorization policies include:

- Identity source and failure options as results for identity policies. See [Authorization Profiles for Network Access, page 3-16](#).
- Identity groups for group mapping. See [Group Mapping Policy, page 3-10](#).
- [Authorization Profiles for Network Access, page 3-16](#).
- [Authorization Policy for Device Administration, page 3-11](#).
- Security groups and security group access control lists (ACLs) for Cisco Security Group Access. See [ACS and Cisco Security Group Access, page 4-22](#).

For additional policy results, see [Managing Authorizations and Permissions, page 9-17](#).

Related Topics

- [Policy Terminology, page 3-2](#)
- [Policy Conditions, page 3-15](#)
- [Exception Authorization Policy Rules, page 3-11](#)
- [Policies and Identity Attributes, page 3-17](#)

Authorization Profiles for Network Access

Authorization profiles define the set of RADIUS attributes that ACS returns to a user after successful authorization. The access authorization information includes authorization privileges and permissions, and other information such as downloadable ACLs.

You can define multiple authorization profiles as a network access policy result. In this way, you maintain a smaller number of authorization profiles, because you can use the authorization profiles in combination as rule results, rather than maintaining all the combinations themselves in individual profiles.

Processing Rules with Multiple Authorization Profiles

A session authorization policy can contain rules with multiple authorization profiles. The authorization profile contains general information (name and description) and RADIUS attributes only. When you use multiple authorization profiles, ACS merges these profiles into a single set of attributes. If a specific attribute appears:

- In only one of the resulting authorization profiles, it is included in the authorization result.
- Multiple times in the result profiles, ACS determines the attribute value for the authorization result based on the attribute value in the profile that appears first in the result set.

For example, if a VLAN appears in the first profile, that takes precedence over a VLAN that appears in a 2nd or 3rd profile in the list.



Note If you are using multiple authorization profiles, make sure you order them in priority order.

The RADIUS attribute definitions in the protocol dictionary specify whether the attribute can appear only once in the response, or multiple times. In either case, ACS takes the values for any attribute from only one profile, irrespective of the number of times the values appear in the response. The only exception is the Cisco attribute value (AV) pair, which ACS takes from all profiles included in the result.

Related Topics

- [Policy Terminology, page 3-2](#)
- [Authorization Policy for Device Administration, page 3-11](#)

Policies and Identity Attributes

The identity stores contain identity attributes that you can use as part of policy conditions and in authorization results. When you create a policy, you can reference the identity attributes and user attributes.

This gives you more flexibility in mapping groups directly to permissions in authorization rules. When ACS processes a request for a user or host, the identity attributes are retrieved and can then be used in authorization policy conditions.

For example, if you are using the ACS internal users identity store, you can reference the identity group of the internal user or you can reference attributes of the internal user. (Note that ACS allows you to create additional custom attributes for the internal identity store records.)

If you are using an external Active Directory (AD), you can reference AD groups directly in authorization rules, and you can also reference AD user attributes directly in authorization rules. User attributes might include a user's department or manager attribute.

Related Topics

- [Managing Users and Identity Stores, page 8-1](#)
- [Policy Terminology, page 3-2](#)
- [Types of Policies, page 3-4](#)

Policies and Network Device Groups

You can reference Network device groups (NDGs) as policy conditions. When the ACS receives a request for a device, the NDGs associated with that device are retrieved and compared against those in the policy table. With this method, you can group multiple devices and assign them the same policies. For example, you can group all devices in a specific location together and assign to them the same policy.

When ACS receives a request from a network device to access the network, it searches the network device repository to find an entry with a matching IP address. When a request arrives from a device that ACS identified using the IP address, ACS retrieves all NDGs associated with the device.

Related Topics

- [Managing Users and Identity Stores, page 8-1](#)
- [Policy Terminology, page 3-2](#)

- [Types of Policies, page 3-4](#)

Example of a Rule-Based Policy

The following example illustrates how you can use policy elements to create policy rules.

A company divides its network into two regions, East and West, with network operations engineers at each site. They want to create an access policy that allows engineers:

- Full access to the network devices in their region.
- Read-only access to devices outside their region.

You can use the ACS 5.8.1 policy model to:

- Define East and West network device groups, and map network devices to the appropriate group.
- Define East and West identity groups, and map users (network engineers) to the appropriate group.
- Define Full Access and Read Only authorization profiles.
- Define Rules that allow each identity group full access or read-only access, depending on the network device group location.

Previously, you had to create two user groups, one for each location of engineers, each with separate definitions for permissions, and so on. This definition would not provide the same amount of flexibility and granularity as in the rule-based model.

[Figure 3-2](#) illustrates what this policy rule table could look like.

Figure 3-2 Sample Rule-Based Policy

g... / ... /

Each row in the policy table represents a single rule.

Each rule, except for the last Default rule, contains two conditions, ID Group and Location, and a result, Authorization Profile. ID Group is an identity-based classification and Location is a nonidentity condition. The authorization profiles contain permissions for a session.

The ID Group, Location, and Authorization Profile are the policy elements.

Related Topics

- [Policy Terminology, page 3-2](#)
- [Types of Policies, page 3-4](#)
- [Access Services, page 3-5](#)
- [Flows for Configuring Services and Policies, page 3-19](#)

Flows for Configuring Services and Policies

[Table 3-9](#) describes the recommended basic flow for configuring services and policies; this flow does not include user-defined conditions and attribute configurations. With this flow, you can use NDGs, identity groups, and compound conditions in rules.

Prerequisites

Before you configure services and policies, it is assumed you have done the following:

- Added network resources to ACS and create network device groups. See [Creating, Duplicating, and Editing Network Device Groups, page 7-2](#) and [Network Devices and AAA Clients, page 7-5](#).
- Added users to the internal ACS identity store or add external identity stores. See [Creating Internal Users, page 8-13](#), [Managing Identity Attributes, page 8-7](#), or [Creating External LDAP Identity Stores, page 8-34](#).

Table 3-9 *Steps to Configure Services and Policies*

Step	Action	Drawer in Web Interface
Step 1	Define policy results: <ul style="list-style-type: none"> • Authorizations and permissions for device administration—Shell profiles or command sets. • Authorizations and permissions for network access—Authorization profile. See: <ul style="list-style-type: none"> • Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-23 • Creating, Duplicating, and Editing Command Sets for Device Administration, page 9-28 • Creating, Duplicating, and Editing Authorization Profiles for Network Access, page 9-18 	Policy Elements
Step 2	(Optional) Define custom conditions to policy rules. You can complete this step before defining policy rules in Step 6, or you can define custom conditions while in the process of creating a rule. See Creating, Duplicating, and Editing a Custom Session Condition, page 9-5 .	—
Step 3	Create Access Services—Define only the structure and allowed protocols; you do not need to define the policies yet. See Creating, Duplicating, and Editing Access Services, page 10-12 .	Access Policies

Table 3-9 *Steps to Configure Services and Policies (continued)*

Step	Action	Drawer in Web Interface
Step 5	Add rules to Service Selection Policy to determine which access service to use for requests. See: <ul style="list-style-type: none">• Customizing a Policy, page 10-4• Creating, Duplicating, and Editing Service Selection Rules, page 10-8	Access Policies
Step 6	Define identity policy. Select the identity store or sequence you want to use to authenticate requests and obtain identity attributes. See Managing Users and Identity Stores, page 8-1 .	Users and Identity Stores
Step 7	Create authorization rules: <ul style="list-style-type: none">• Device administration—Shell/command authorization policy.• Network access—Session authorization policy. See: <ul style="list-style-type: none">• Customizing a Policy, page 10-4• Configuring Access Service Policies, page 10-23	Access Policies

Related Topics

- [Policy Terminology, page 3-2](#)
- [Policy Conditions, page 3-15](#)
- [Policy Results, page 3-16](#)
- [Policies and Identity Attributes, page 3-17](#)



Common Scenarios Using ACS

Network control refers to the process of controlling access to a network. Traditionally a username and password was used to authenticate a user to a network. Now a days with the rapid technological advancements, the traditional method of managing network access with a username and a password is no longer sufficient.

The ways in which the users can access the network and what they can access have changed considerably. Hence, you must define complex and dynamic policies to control access to your network.

For example, earlier, a user was granted access to a network and authorized to perform certain actions based on the group that the user belonged to. Now, in addition to the group that the user belongs to, you must also consider other factors, such as whether:

- The user is trying to gain access within or outside of work hours.
- The user is attempting to gain access remotely.
- The user has full or restricted access to the services and resources.

Apart from users, you also have devices that attempt to connect to your network.

When users and devices try to connect to your network through network access servers, such as wireless access points, 802.1x switches, and VPN servers, ACS authenticates and authorizes the request before a connection is established.

Authentication is the process of verifying the identity of the user or device that attempts to connect to a network. ACS receives identity proof from the user or device in the form of credentials. There are two different authentication methods:

- Password-based authentication—A simpler and easier way of authenticating users. The user enters a username and password. The server checks for the username and password in its internal or external databases and if found, grants access to the user. The level of access (authorization) is defined by the rules and conditions that you have created.
- Certificate-based authentication—ACS supports certificate-based authentication with the use of the Extensible Authentication Protocol-Transport Level Security (EAP-TLS) and Protected Extensible Authentication Protocol-Transport Level Security (PEAP-TLS), which uses certificates for server authentication by the client and for client authentication by the server.

Certificate-based authentication methods provide stronger security and are recommended when compared to password-based authentication methods.

Authorization determines the level of access that is granted to the user or device. The rule-based policy model in ACS 5.x allows you to define complex conditions in rules. ACS uses a set of rules (policy) to evaluate an access request and to return a decision.

ACS organizes a sequence of independent policies into an access service, which is used to process an access request. You can create multiple access services to process different kinds of access requests; for example, for device administration or network access.

Cisco Secure Access Control System (ACS) allows you to centrally manage access to your network services and resources (including devices, such as IP phones, printers, and so on). ACS 5.8.1 is a policy-based access control system that allows you to create complex policy conditions and helps you to comply with the various Governmental regulations.

When you deploy ACS in your network, you must choose an appropriate authentication method that determines access to your network.

This chapter provides guidelines for some of the common scenarios. This chapter contains:

- [Overview of Device Administration, page 4-2](#)
- [Password-Based Network Access, page 4-5](#)
- [Certificate-Based Network Access, page 4-8](#)
- [Agentless Network Access, page 4-12](#)
- [VPN Remote Network Access, page 4-20](#)
- [ACS and Cisco Security Group Access, page 4-22](#)
- [RADIUS and TACACS+ Proxy Requests, page 4-27](#)
- [FIPS 140-2 Level 1 Implementation, page 4-35](#)
- [Enabling and Disabling IPv6 for Network Interfaces, page 4-37](#)

Overview of Device Administration

Device administration allows ACS to control and audit the administration operations performed on network devices, by using these methods:

- Session administration—A session authorization request to a network device elicits an ACS response. The response includes a token that is interpreted by the network device which limits the commands that may be executed for the duration of a session. See [Session Administration, page 4-3](#).
- Command authorization—When an administrator issues operational commands on a network device, ACS is queried to determine whether the administrator is authorized to issue the command. See [Command Authorization, page 4-4](#).

Device administration results can be shell profiles or command sets.

Shell profiles allow a selection of attributes to be returned in the response to the authorization request for a session, with privilege level as the most commonly used attribute. Shell profiles contain common attributes that are used for shell access sessions and user-defined attributes that are used for other types of sessions.

ACS 5.8.1 allows you to create custom TACACS+ authorization services and attributes. You can define:

- Any A-V pairs for these attributes.
- The attributes as either optional or mandatory.
- Multiple A-V pairs with the same name (multi-part attributes).

ACS also supports task-specific predefined shell attributes. Using the TACACS+ shell profile, you can specify custom attributes to be returned in the shell authorization response. See [TACACS+ Custom Services and Attributes, page 4-4](#).

Command sets define the set of commands, and command arguments, that are permitted or denied. The received command, for which authorization is requested, is compared against commands in the available command sets that are contained in the authorization results.

If a command is matched to a command set, the corresponding permit or deny setting for the command is retrieved. If multiple results are found in the rules that are matched, they are consolidated and a single permit or deny result for the command is returned, as described in these conditions:

- If an explicit deny-always setting exists in any command set, the command is denied.
- If no explicit deny-always setting exists in a command set, and any command set returns a permit result, the command is permitted.
- If either of the previous two conditions are not met, the command is denied.

You configure the permit and deny settings in the device administration rule table. You configure policy elements within a device administration rule table as conditions that are or not met. The rule table maps specific request conditions to device administration results through a matching process. The result of rule table processing is a shell profile or a command set, dependent on the type of request.

Session administration requests have a shell profile result, which contains values of attributes that are used in session provisioning. Command authorization requests have a command authorization result, which contains a list of command sets that are used to validate commands and arguments.

This model allows you to configure the administrator levels to have specific device administration capabilities. For example, you can assign a user the Network Device Administrator role which provides full access to device administration functions, while a Read Only Admin cannot perform administrative functions.

Session Administration

The following steps describe the flow for an administrator to establish a session (the ability to communicate) with a network device:

- Step 1** An administrator accesses a network device.
- Step 2** The network device sends a RADIUS or TACACS+ access request to ACS.
- Step 3** ACS uses an identity store (external LDAP, Active Directory, RSA, RADIUS Identity Server, or internal ACS identity store) to validate the administrator's credentials.
- Step 4** The RADIUS or TACACS+ response (accept or reject) is sent to the network device. The accept response also contains the administrator's maximum privilege level, which determines the level of administrator access for the duration of the session.

To configure a session administration policy (device administration rule table) to permit communication:

- Step 1** Configure the TACACS+ protocol global settings and user authentication option. See [Configuring TACACS+ Settings, page 18-1](#).
- Step 2** Configure network resources. See [Network Devices and AAA Clients, page 7-5](#).
- Step 3** Configure the users and identity stores. See [Managing Internal Identity Stores, page 8-4](#) or [Managing External Identity Stores, page 8-29](#).
- Step 4** Configure shell profiles according to your needs. See [Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-23](#).
- Step 5** Configure an access service policy. See [Access Service Policy Creation, page 10-4](#).

- Step 6** Configure a service selection policy. See [Service Selection Policy Creation, page 10-4](#).
- Step 7** Configure an authorization policy (rule table). See [Configuring a Session Authorization Policy for Network Access, page 10-31](#).

Command Authorization

This topic describes the flow for an administrator to issue a command to a network device.

- Note** The device administration command flow is available for the TACACS+ protocol only.
- Step 1** An administrator issues a command to a network device.
- Step 2** The network device sends an access request to ACS.
- Step 3** ACS optionally uses an identity store (external Lightweight Directory Access Protocol [LDAP], Active Directory, RADIUS Identity Server, or internal ACS identity store) to retrieve user attributes which are included in policy processing.
- Step 4** The response indicates whether the administrator is authorized to issue the command.
- Step 5** To configure a command authorization policy (device administration rule table) to allow an administrator to issue commands to a network device:
- Step 6** Configure the TACACS+ protocol global settings and user authentication option. See [Configuring TACACS+ Settings, page 18-1](#).
- Step 7** Configure network resources. See [Network Devices and AAA Clients, page 7-5](#).
- Step 8** Configure the users and identity stores. See [Managing Internal Identity Stores, page 8-4](#) or [Managing External Identity Stores, page 8-29](#).
- Step 9** Configure command sets according to your needs. See [Creating, Duplicating, and Editing Command Sets for Device Administration, page 9-28](#).
- Step 10** Configure an access service policy. See [Access Service Policy Creation, page 10-4](#).
- Step 11** Configure a service selection policy. See [Service Selection Policy Creation, page 10-4](#).
- Step 12** Configure an authorization policy (rule table). See [Configuring Shell/Command Authorization Policies for Device Administration, page 10-36](#).

Related Topics

- [Network Devices and AAA Clients, page 7-5](#)
- [Configuring System Administrators and Accounts, page 16-3](#)
- [Managing Users and Identity Stores, page 8-1](#)
- [Managing External Identity Stores, page 8-29](#)
- [Managing Policy Conditions, page 9-1](#)
- [Managing Access Policies, page 10-1](#)

TACACS+ Custom Services and Attributes

This topic describes the configuration flow to define TACACS+ custom attributes and services.

- Step 1** Create a custom TACACS+ condition to move to TACACS+ service on request. To do this:
- Go to **Policy Elements > Session Conditions > Custom** and click **Create**.
 - Create a custom TACACS+ condition. See [Creating, Duplicating, and Editing a Custom Session Condition, page 9-5](#).
- Step 2** Create an access service for Device Administration with the TACACS+ shell profile as the result. See [Configuring Shell/Command Authorization Policies for Device Administration, page 10-36](#).
- Step 3** Create custom TACACS+ attributes. See [Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-23](#).

Password-Based Network Access

This section contains the following topics:

- [Overview of Password-Based Network Access, page 4-5](#)
- [Password-Based Network Access Configuration Flow, page 4-6](#)

For more information about password-based protocols, see [Authentication in ACS 5.8.1, page C-1](#)

Overview of Password-Based Network Access

The use of a simple, unencrypted username and password is not considered a strong authentication mechanism but can be sufficient for low authorization or privilege levels such as Internet access.

Encryption reduces 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 AAA client and ACS. Before this point in the authentication process, unauthorized persons can obtain clear-text passwords, in these scenarios:

- The communication between an end-user client dialing up over a phone line
- An ISDN line terminating at a network-access server
- Over a Telnet session between an end-user client and the hosting device

ACS supports various authentication methods for authentication against the various identity stores that ACS supports. For more information about authentication protocol identity store compatibility, see [Authentication Protocol and Identity Store Compatibility, page C-36](#).

Passwords can be processed by using these password-authentication protocols based on the version and type of security-control protocol used (for example, RADIUS), and the configuration of the AAA client and end-user client.

You can use different levels of security with ACS concurrently, for different requirements. Password Authentication Protocol (PAP) provides a basic security level. PAP provides a very basic level of security, but is simple and convenient for the client. MSCHAPv2 allows a higher level of security for encrypting passwords when communicating from an end-user client to the AAA client.

Note During password-based access (or certificate-based access), the user is not only authenticated but also *authorized* according to the ACS configuration. And if NAS sends accounting requests, the user is also accounted.

ACS supports the following password-based authentication methods:

- Plain RADIUS password authentication methods

- RADIUS-PAP
- RADIUS-CHAP
- RADIUS-MSCHAPv1
- RADIUS-MSCHAPv2
- RADIUS EAP-based password authentication methods
 - PEAP-MSCHAPv2
 - PEAP-GTC
 - EAP-FAST-MSCHAPv2
 - EAP-FAST-GTC
 - EAP-MD5
 - LEAP

You must choose the authentication method based on the following factors:

- The network access server—Wireless access points, 802.1X authenticating switches, VPN servers, and so on.
- The client computer and software—EAP supplicant, VPN client, and so on.
- The identity store that is used to authenticate the user—Internal or External (AD, LDAP, RSA token server, or RADIUS identity server).

Related Topics

- [Authentication in ACS 5.8.1, page C-1](#)
- [Password-Based Network Access Configuration Flow, page 4-6](#)
- [Network Devices and AAA Clients, page 7-5](#)
- [Managing Access Policies, page 10-1](#)

Password-Based Network Access Configuration Flow

This topic describes the end-to-end flow for password-based network access and lists the tasks that you must perform. The information about how to configure the tasks is located in the relevant task chapters.

To configure password-based network access:

- Step 1** Configure network devices and AAA clients.
 - a. In the [Network Devices and AAA Clients, page 7-5](#), configure the **Authentication Setting** as RADIUS.
 - b. Enter the Shared Secret.
See [Network Devices and AAA Clients, page 7-5](#), for more information.
- Step 2** Configure the users and identity stores. For more information, see [Managing Users and Identity Stores, page 8-1](#).
- Step 3** Define policy conditions and authorization profiles. For more information, see [Managing Policy Elements, page 9-1](#)

- Step 4** Define an access service. For more information, see [Creating, Duplicating, and Editing Access Services, page 10-12](#).
- Set the Access Service Type to Network Access.
 - Select one of the ACS-supported protocols in the Allowed Protocols Page and follow the steps in the Action column in [Table 4-1](#).
- Note** If ACS is set to operate in FIPS mode, some protocols are not supported. For more information, see [FIPS 140-2 Level 1 Implementation, page 4-35](#).
- Step 5** Add the access service to your service selection policy. For more information, see [Creating, Duplicating, and Editing Service Selection Rules, page 10-8](#).
- Step 6** Return to the service that you created and in the Authorization Policy Page, define authorization rules. For more information, see [Configuring Access Service Policies, page 10-23](#).

Table 4-1 Network Access Authentication Protocols

Protocol	Action
Process Host Lookup (MAB)	In the Allowed Protocols Page, choose Process Host Lookup .
RADIUS PAP	In the Allowed Protocols Page, choose Allow PAP/ASCII .
RADIUS CHAP	In the Allowed Protocols Page, choose Allow CHAP .
RADIUS MSCHAPv1	In the Allowed Protocols Page, choose Allow MS-CHAPv1 .
RADIUS MSCHAPv2	In the Allowed Protocols Page, choose Allow MS-CHAPv2 .
EAP-MD5	In the Allowed Protocols Page, choose Allow EAP-MD5 .
LEAP	In the Allowed Protocols Page, choose Allow LEAP .
PEAP	In the Allowed Protocols Page, choose PEAP . For the PEAP inner method, choose EAP-MSCHAPv2 or EAP-GTC or both.
EAP-FAST	<ol style="list-style-type: none"> In the Allowed Protocols Page, choose Allow EAP-FAST to enable the EAP-FAST settings. For the EAP-FAST inner method, choose EAP-MSCHAPv2 or EAP-GTC or both. Select Allow Anonymous In-Band PAC Provisioning or Allow Authenticated In-Band PAC Provisioning or both. For Windows machine authentication against Microsoft AD and for the change password feature: <ol style="list-style-type: none"> Click the Use PACS radio button. For details about PACs, see About PACs, page C-22. Check Allow Authenticated In-Band PAC Provisioning. Check Allow Machine Authentication. Enter the Machine PAC Time to Live. Check Enable Stateless Session Resume. Enter the Authorization PAC Time to Live. Check Preferred EAP Protocol to set the preferred protocol from the list. Check EAP-TLS L-bit to set the Length included flag in the access policies.

For RADIUS, non-EAP authentication methods (RADIUS/PAP, RADIUS/CHAP, RADIUS/MS-CHAPv1, RADIUS/MSCHAPv2), and simple EAP methods (EAP-MD5 and LEAP), you need to configure only the protocol in the Allowed Protocols page as defined in [Table 4-1](#).

Some of the complex EAP protocols require additional configuration:

- For EAP-TLS, you must also configure:
 - The EAP-TLS settings under **System Administration > Configuration > EAP-TLS Settings**.
 - A local server certificate under **System Administration > Configuration > Local Server Certificates > Local Certificates**.
 - A CA certificate under **Users and Identity Stores > Certificate Authorities**.
- For PEAP, you must also configure:
 - The inner method in the Allowed Protocols page and specify whether password change is allowed.
 - The PEAP settings under **System Administration > Configuration > PEAP Settings**.
 - Local server certificates under **System Administration > Configuration > Local Server Certificates > Local Certificates**.
- For EAP-FAST, you must also configure:
 - The inner method in the Allowed Protocols page and specify whether password change is allowed.
 - Whether or not to use PACs and if you choose to use PACs, you must also specify how to allow in-band PAC provisioning.
 - The EAP-FAST settings under **System Administration > Configuration > EAP-FAST > Settings**.
 - A local server certificate under **System Administration > Configuration > Local Server Certificates > Local Certificates** (Only if you enable authenticated PAC provisioning).

Related Topics

- [Authentication in ACS 5.8.1, page C-1](#)
- [Network Devices and AAA Clients, page 7-5](#)
- [Managing Access Policies, page 10-1](#)
- [Creating, Duplicating, and Editing Access Services, page 10-12](#)
- [About PACs, page C-22](#)

Certificate-Based Network Access

This section contains the following topics:

- [Overview of Certificate-Based Network Access, page 4-9](#)
- [Using Certificates in ACS, page 4-10](#)
- [Certificate-Based Network Access, page 4-10](#)

For more information about certificate-based protocols, see [Authentication in ACS 5.8.1, page C-1](#)

Overview of Certificate-Based Network Access

Before using EAP-TLS, you must install a computer certificate on ACS. The installed computer certificate must be issued from a CA that can follow a certificate chain to a root CA that the access client trusts.

Additionally, in order for ACS to validate the user or computer certificate of the access client, you must install the certificate of the root CA that issued the user or computer certificate to the access clients.

ACS supports certificate-based network access through the EAP-TLS protocol, which uses certificates for server authentication by the client and for client authentication by the server.

Other protocols, such as PEAP or the authenticated-provisioning mode of EAP-FAST also make use of certificates for server authentication by the client, but they cannot be considered certificate-based network access because the server does not use the certificates for client authentication.

ACS Public Key Infrastructure (PKI) certificate-based authentication is based on X509 certificate identification. The entity which identifies itself with a certificate holds a private-key that correlates to the public key stored in the certificate.

A certificate can be self-signed or signed by another CA. A hierarchy of certificates can be made to form trust relations of each entity to its CA. The trusted root CA is the entity that signs the certificate of all other CAs and eventually signs each certificate in its hierarchy.

ACS identifies itself with its own certificate. ACS supports a certificate trust list (CTL) for authorizing connection certificates. ACS also supports complex hierarchies that authorize an identity certificate when all of the chain certificates are presented to it.

ACS supports several RSA key sizes used in the certificate that are 512, 1024, 2048, or 4096 bits. Other key sizes may be used. ACS 5.8.1 supports RSA. ACS does not support the Digital Signature Algorithm (DSA). However, in some use cases, ACS will not prevent DSA cipher suites from being used for certificate-based authentication.

All certificates that are used for network access authentication must meet the requirements for X.509 certificates and work for connections that use SSL/TLS. After this minimum requirement is met, the client and server certificates have additional requirements.

You can configure two types of certificates in ACS:

- Trust certificate—Also known as CA certificate. Used to form CTL trust hierarchy for verification of remote certificates.
- Local certificate—Also known as local server certificate. The client uses the local certificate with various protocols to authenticate the ACS server. This certificate is maintained in association with its private key, which is used to prove possession of the certificate.
- During certificate-based access (or password-based access), the user is not only authenticated but also *authorized* according to the ACS configuration. And if NAS sends accounting requests, the user is also accounted.

Note ACS does not support wild card certificates.

Related Topics

- [Configuring CA Certificates, page 8-95](#)
- [Configuring Local Server Certificates, page 18-16](#)
- [Using Certificates in ACS, page 4-10](#)

Using Certificates in ACS

The three use cases for certificates in ACS 5.8.1 are:

- [Certificate-Based Network Access, page 4-10](#)
- [Authorizing the ACS Web Interface from Your Browser Using a Certificate, page 4-11](#)
- [Validating an LDAP Secure Authentication Connection, page 4-11](#)

Certificate-Based Network Access

For TLS- related EAP and PEAP protocols, you must set up a server certificate from the local certificate store and a trust list certificate to authenticate the client. You can choose the trust certificate from any of the certificates in the local certificate store.

To use EAP-TLS, EAP-FAST (EAP-TLS), or PEAP (EAP-TLS), you must obtain and install trust certificates. The information about how to perform the tasks is located in the relevant task chapters.

Before you Begin:

Set up the server by configuring:

- EAP-TLS or PEAP (EAP-TLS)
- The local certificate. See [Configuring Local Server Certificates, page 18-16](#).

To configure certificate-based network access for EAP-TLS or PEAP (EAP-TLS):

- Step 1** Configure the trust certificate list. See [Configuring CA Certificates, page 8-95](#), for more information.
- Step 2** Configure the LDAP external identity store. You might want to do this to verify the certificate against a certificate stored in LDAP. See [Creating External LDAP Identity Stores, page 8-34](#), for details.
- Step 3** Set up the Certificate Authentication Profile. See [Configuring Certificate Authentication Profiles, page 8-99](#), for details.
- Step 4** Configure policy elements. See [Managing Policy Conditions, page 9-1](#), for more information.
- Step 5** You can create custom conditions to use the certificate's attributes as a policy condition. See [Creating, Duplicating, and Editing a Custom Session Condition, page 9-5](#), for details.
- Step 6** Create an access service. See [Configuring Access Services, page 10-11](#), for more information.
- Step 7** In the Allowed Protocols Page, choose **EAP-TLS or PEAP (EAP-TLS)** as inner method.
- Step 8** Configure identity and authorization policies for the access service. See [Configuring Access Service Policies, page 10-23](#), for details.

Note When you create rules for the identity policy, the result may be the Certificate Authentication Profile or an Identity Sequence. See [Viewing Identity Policies, page 10-23](#), for more information.
- Step 9** Configure the Authorization Policies. See [Configuring a Session Authorization Policy for Network Access, page 10-31](#).
- Step 10** Configure the Service Selection Policy. See [Configuring the Service Selection Policy, page 10-5](#).

Table 4-2 Network Access Authentication Protocols

Protocol	Action
EAP-TLS	<p>In the Allowed Protocols Page, choose Allow EAP-TLS to enable the EAP-TLS settings.</p> <ul style="list-style-type: none"> • Enable Stateless Session resume—Check this check box to enable the Stateless Session Resume feature per Access service. This feature enables you to configure the following options: <ul style="list-style-type: none"> – Proactive Session Ticket update—Enter the value as a percentage to indicate how much of the Time to Live must elapse before the session ticket is updated. For example, the session ticket update occurs after 10 percent of the Time to Live has expired, if you enter the value 10. – Session ticket Time to Live—Enter the equivalent maximum value in days, weeks, months, and years, using a positive integer.
PEAP	<p>In the Allowed Protocols Page, choose PEAP. For the PEAP inner method, choose EAP-TLS or PEAP Cryptobinding TLV.</p>

Related Topics

- [Configuring Local Server Certificates, page 18-16](#)
- [Configuring CA Certificates, page 8-95](#)
- [Authentication in ACS 5.8.1, page C-1](#)
- [Overview of EAP-TLS, page C-6](#)

Authorizing the ACS Web Interface from Your Browser Using a Certificate

You use the HTTPS certificate-based authentication to connect to ACS with your browser. The Local Server Certificate in ACS is used to authorize the ACS web interface from your browser. ACS does not support browser authentication (mutual authentication is not supported).

A default Local Server Certificate is installed on ACS so that you can connect to ACS with your browser. The default certificate is a self-signed certificate and cannot be modified during installation.

Related Topics

- [Using Certificates in ACS, page 4-10](#)
- [Configuring Local Server Certificates, page 18-16](#)

Validating an LDAP Secure Authentication Connection

You can define a secure authentication connection for the LDAP external identity store, by using a CA certificate to validate the connection.

To validate an LDAP secure authentication connection using a certificate:

- Step 1** Configure an LDAP external identity store. See [Creating External LDAP Identity Stores, page 8-34](#).
- Step 2** In the LDAP Server Connection page, check **Use Secure Authentication**.
- Step 3** Select **Root CA** from the drop-down menu and continue with the LDAP configuration for ACS.

Related Topics

- [Using Certificates in ACS, page 4-10](#)
- [Configuring Local Server Certificates, page 18-16](#)
- [Managing External Identity Stores, page 8-29](#)

Agentless Network Access

This section contains the following topics:

- [Overview of Agentless Network Access, page 4-12](#)
- [Host Lookup, page 4-12](#)
- [Agentless Network Access Flow, page 4-15](#)

For more information about protocols used for network access, see [Authentication in ACS 5.8.1, page C-1](#).

Overview of Agentless Network Access

Agentless network access refers to the mechanisms used to perform port-based authentication and authorization in cases where the host device does not have the appropriate agent software.

For example, a host device, where there is no 802.1x supplicant or a host device, where the supplicant is disabled.

802.1x must be enabled on the host device and on the switch to which the device connects. If a host/device without an 802.1x supplicant attempts to connect to a port that is enabled for 802.1x, it will be subjected to the default security policy.

The default security policy says that 802.1x authentication must succeed before access to the network is granted. Therefore, by default, non-802.1x-capable devices cannot get access to an 802.1x-protected network.

Although many devices increasingly support 802.1x, there will always be devices that require network connectivity, but do not, or cannot, support 802.1x. Examples of such devices include network printers, badge readers, and legacy servers. You must make some provision for these devices.

Cisco provides two features to accommodate non-802.1x devices. For example, MAC Authentication Bypass (Host Lookup) and the Guest VLAN access by using web authentication.

ACS 5.8.1 supports the Host Lookup fall back mechanism when there is no 802.1x supplicant. After 802.1x times out on a port, the port can move to an open state if Host Lookup is configured and succeeds.

Related Topics

- [Host Lookup, page 4-12](#)
- [Agentless Network Access Flow, page 4-15](#)

Host Lookup

ACS uses Host Lookup as the validation method when an identity cannot be authenticated according to credentials (for example, password or certificate), and ACS needs to validate the identity by doing a lookup in the identity stores.

An example for using host lookup is when a network device is configured to request MAC Authentication Bypass (MAB). This can happen after 802.1x times out on a port or if the port is explicitly configured to perform authentication bypass. When MAB is implemented, the host connects to the network access device.

The device detects the absence of the appropriate software agent on the host and determines that it must identify the host according to its MAC address. The device sends a RADIUS request with *service-type=10* and the MAC address of the host to ACS in the calling-station-id attribute.

Some devices might be configured to implement the MAB request by sending PAP or EAP-MD5 authentication with the MAC address of the host in the user name, user password, and CallingStationID attributes, but without the *service-type=10* attribute.

While most use cases for host lookup are to obtain a MAC address, there are other scenarios where a device requests to validate a different parameter, and the calling-station-id attribute contains this value instead of the MAC address. For example, IP address in layer 3 use cases).

Table 4-3 describes the RADIUS parameters required for host lookup use cases.

Table 4-3 *RADIUS Attributes for Host Lookup Use Cases*

Attribute	Use Cases		
	PAP	802.1x	EAP-MD5
RADIUS::ServiceType	—	Call check (with PAP or EAP-MD5)	—
RADIUS::UserName	MAC address	Any value (usually the MAC address)	MAC address
RADIUS::UserPassword	MAC address	Any value (usually the MAC address)	MAC address
RADIUS::CallingStationID	MAC address	MAC address	MAC address

ACS supports host lookup for the following identity stores:

- Internal hosts
- External LDAP
- Internal users
- Active Directory

You can access the Active Directory via the LDAP API.

You can use the Internal Users identity store for Host Lookup in cases where the relevant host is already listed in the Internal Users identity store, and you prefer not to move the data to the Internal Hosts identity store.

ACS uses the MAC format (XX-XX-XX-XX-XX-XX) and no other conversions are possible. To search the Internal Users identity store using the User-Name attribute (for example, xx:xx:xx:xx:xx:xx) you should leave the Process Host Lookup option unchecked. ACS will handle the request as a PAP request.

When MAC address authentication over PAP or EAP-MD5 is not detected according to the Host Lookup configuration, authentication and authorization occur like regular user authentication over PAP or EAP-MD5. You can use any identity store that supports these authentication protocols. ACS uses the MAC address format as presented in the RADIUS User-Name attribute.

Related Topics

- [Creating an Access Service for Host Lookup, page 4-18](#)
- [Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-25](#)
- [Managing Users and Identity Stores, page 8-1](#)
- [Authentication with Call Check, page 4-14](#)

Authentication with Call Check

When ACS identifies a network access request with the call check attribute as Host Lookup (RADIUS::ServiceType = 10), ACS authenticates (validates) and authorizes the host by looking up the value in the Calling-Station-ID attribute (for example, the MAC address) in the configured identity store according to the authentication policy.

When ACS receives a RADIUS message, it performs basic parsing and validation, and then checks if the Call Check attribute, RADIUS ServiceType(6), is equal to the value 10. If the RADIUS ServiceType is equal to 10, ACS sets the system dictionary attribute UseCase to a value of Host Lookup.

In the ACS packet processing flow, the detection of Host Lookup according to Call Check service-type is done before the service selection policy. It is possible to use the condition *UseCase equals Host Lookup* in the service selection policy.

Initially, when RADIUS requests are processed, the RADIUS User-Name attribute is copied to the System UserName attribute. When the RADIUS Service-Type equals 10, the RADIUS Calling-Station-ID attribute is copied to the System User-Name attribute, and it overrides the RADIUS User-Name attribute value.

ACS supports four MAC address formats:

- Six groups of two hexadecimal digits, separated by hyphens—01-23-45-67-89-AB
- Six groups of two hexadecimal digits, separated by colons—01:23:45:67:89:AB
- Three groups of four hexadecimal digits, separated by dots—0123.4567.89AB
- Twelve consecutive hexadecimal digits without any separators—0123456789AB

If the Calling-Station-ID attribute is one of the four supported MAC address formats above, ACS copies it to the User-Name attribute with the format of XX-XX-XX-XX-XX-XX. If the MAC address is in a format other than one of the four above, ACS copies the string as is.

Process Service-Type Call Check

You may not want to copy the CallingStationID attribute value to the System UserName attribute value. When the Process Host Lookup option is checked, ACS uses the System UserName attribute that was copied from the RADIUS User-Name attribute.

When the Process Host Lookup option is not checked, ACS ignores the HostLookup field and uses the original value of the System UserName attribute for authentication and authorization. The request processing continues according to the message protocol. For example, according to the RADIUS User-Name and User-Password attributes for PAP.

For setting the Process Host Lookup option, see [Creating an Access Service for Host Lookup, page 4-18](#).

PAP/EAP-MD5 Authentication

When a device is configured to use PAP or EAP-MD5 for MAC address authentication, you can configure ACS to detect the request as a Host Lookup request, within the network access service. The device sends the request with the host's MAC address in the User-Name, User-Password, and Calling-Station-ID attributes.

If you do not configure ACS to detect Host Lookup, the access request is handled as a regular PAP, or EAP-MD5 authentication request.

If you check the Process HostLookup field and select PAP or EAP-MD5, ACS places the HostLookup value in the ACS::UseCase attribute. The User-Password attribute is ignored for the detection algorithm.

ACS follows the authentication process as if the request is using the call check attribute, and processes it as a Host Lookup (Service-Type=10) request. The RADIUS dictionary attribute ACS::UseCase is set to the value of HostLookup.

The Detect Host Lookup option for PAP and EAP-MD5 MAC authentication is done after the service selection policy. If a service selection rule is configured to match ACS::UseCase = Host Lookup, the request falls into the Host Lookup category.

If ACS is not configured to detect PAP or EAP-MD5 authentications as MAC authentication flows, ACS will not consider the Detect Host Lookup option. These requests are handled like a regular user request for authentication, and looks for the username and password in the selected identity store.

Related Topics

- [Creating an Access Service for Host Lookup, page 4-18](#)
- [Managing Access Policies, page 10-1](#)
- [Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-25](#)
- [Managing Users and Identity Stores, page 8-1](#)

Agentless Network Access Flow

This topic describes the end-to-end flow for agentless network access and lists the tasks that you must perform. The information about how to configure the tasks is located in the relevant task chapters.

Perform these tasks in the order listed to configure agentless network access in ACS:

- Step 1** Configure network devices and AAA clients.
- This is the general task to configure network devices and AAA clients in ACS and is not specific to agentless network access.
- Step 2** Select **Network Resources > Network Devices and AAA Clients** and click **Create**. See [Network Devices and AAA Clients, page 7-5](#).
- Step 3** Configure an identity store for internal hosts.
- Configure an internal identity store. See [Adding a Host to an Internal Identity Store, page 4-16](#)
 - or
 - Configure an external identity store. See [Configuring an LDAP External Identity Store for Host Lookup, page 4-17](#).

For more information, see [Managing Users and Identity Stores, page 8-1](#)

- Step 4** Configure the identity group. See [Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17](#).
- For more information, see [Managing Users and Identity Stores, page 8-1](#)
- Step 5** Define policy elements and authorization profiles for Host Lookup requests.
- For more information, see [Managing Policy Elements, page 9-1](#)
- Step 6** Create an empty service by defining an access service for Host Lookup. For more information, see [Creating an Access Service for Host Lookup, page 4-18](#).
- Step 7** Return to the service that you created:
- Define an identity policy. For more information, see [Configuring an Identity Policy for Host Lookup Requests, page 4-18](#).
- ACS has the option to look for host MAC addresses in multiple identity stores.
- For example, MAC addresses can be in the Internal Hosts identity store, in one of the configured LDAP identity stores, or in the Internal Users identity store.
- The MAC address lookup may be in one of the configured identity stores, and the MAC attributes may be fetched from a different identity store that you configured in the identity sequence.
- You can configure ACS to continue processing a Host Lookup request even if the MAC address was not found in the identity store. An administrator can define an authorization policy based on the event, regardless of whether or not the MAC address was found.
- The ACS::UseCase attribute is available for selection in the Authentication Policy, but is not mandatory for Host Lookup support.
- Return to the service that you created.
 - Define an authorization policy. For more information, see [Configuring an Authorization Policy for Host Lookup Requests, page 4-19](#).
- Step 8** Define the service selection.
- Step 9** Add the access service to your service selection policy. For more information, see [Creating, Duplicating, and Editing Service Selection Rules, page 10-8](#).

Related Topics

- [Managing Users and Identity Stores, page 8-1](#)
- [Managing Access Policies, page 10-1](#)

Adding a Host to an Internal Identity Store

To configure an internal identity store for Host Lookup:

- Step 1** Choose **Users and Identity Store > Internal Identity Stores > Hosts** and click **Create**.
- See [Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-25](#), for more information.
- Step 2** Fill in the fields as described in the **Users and Identity Stores > Internal Identity Store > Hosts > Create** Page.
- Step 3** Click **Submit**.

Previous Step:

[Network Devices and AAA Clients, page 7-5](#)

Next Step:

[Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17](#)

Configuring an LDAP External Identity Store for Host Lookup

To configure an LDAP external identity store for Host Lookup:

- Step 1** Choose **Users and Identity Stores > External Identity Stores > LDAP** and click **Create**. See [Creating External LDAP Identity Stores, page 8-34](#), for more information.
- Step 2** Follow the steps for creating an LDAP database.
In the LDAP: Directory Organization page, choose the MAC address format.
The format you choose represents the way MAC addresses are stored in the LDAP external identity store.
- Step 3** Click **Finish**.

Previous Step:

[Network Devices and AAA Clients, page 7-5](#)

Next Step:

[Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17](#)

Related Topics

- [Creating External LDAP Identity Stores, page 8-34](#)
- [Deleting External LDAP Identity Stores, page 8-42](#)

Configuring an Identity Group for Host Lookup Network Access Requests

To configure an identity group for Host Lookup network access requests:

- Step 1** Choose **Users and Identity Store > Identity Groups>** and click **Create**.
See [Managing Identity Attributes, page 8-7](#), for more information.
- Step 2** Fill in the fields as required.
The identity group may be any agentless device, such as a printer or phone.
- Step 3** Click **Submit**.

Previous Steps:

- [Adding a Host to an Internal Identity Store, page 4-16](#)
- [Configuring an LDAP External Identity Store for Host Lookup, page 4-17](#)

Next Step:

- [Creating an Access Service for Host Lookup, page 4-18](#)

Related Topic

- [Managing Identity Attributes, page 8-7](#)

Creating an Access Service for Host Lookup

You create an access service and then enable agentless host processing.

To create an access service for Host Lookup:

- Step 1** Choose **Access Policies > Access Service**, and click **Create**. See [Configuring Access Services, page 10-11](#), for more information.
- Step 2** Fill in the fields as described in the Access Service Properties—General page:
- a. In the Service Structure section, choose **User Selected Policy Structure**.
 - b. Set the Access Service Type to **Network Access** and define the policy structure.
 - c. Select **Network Access**, and check **Identity** and **Authorization**.
The group mapping and External Policy options are optional.
 - d. Make sure you select Process Host Lookup.
If you want ACS to detect PAP or EAP-MD5 authentications for MAC addresses (see [PAP/EAP-MD5 Authentication, page 4-15](#)), and process it like it is a Host Lookup request (for example, MAB requests), complete the following steps:
 - e. Select one of the ACS supported protocols for MAB in the Allowed Protocols Page (EAP-MD5 or PAP).
 - f. Check **Detect PAP/EAP-MD5** as Host Lookup.

Related Topics

- [Managing Access Policies, page 10-1](#)
- [Authentication in ACS 5.8.1, page C-1](#)
- [Authentication with Call Check, page 4-14](#)
- [Process Service-Type Call Check, page 4-14](#)

Configuring an Identity Policy for Host Lookup Requests

To configure an identity policy for Host Lookup requests:

- Step 1** Choose **Access Policies > Access Services > <access_servicename> Identity**.
See [Viewing Identity Policies, page 10-23](#), for details.
- Step 2** Select **Customize** to customize the authorization policy conditions.
A list of conditions appears. This list includes identity attributes, system conditions, and custom conditions. See [Customizing a Policy, page 10-4](#), for more information.
- Step 3** Select **Use Case** from the **Available** customized conditions and move it to the **Selected** conditions.
- Step 4** In the Identity Policy Page, click **Create**.
- a. Enter a **Name** for the rule.
 - b. In the Conditions area, check **Use Case**, then check whether the value should or should not match.

- c. Select **Host Lookup** and click **OK**.

This attribute selection ensures that while processing the access request, ACS will look for the host and not for an IP address.

- d. Select any of the identity stores that support host lookup as your Identity Source.
- e. Click **OK**.

Step 5 Click **Save Changes**.

Related Topic

- [Managing Access Policies, page 10-1](#)

Configuring an Authorization Policy for Host Lookup Requests

To configure an authorization policy for Host Lookup requests:

Step 1 Choose **Access Policies > Access Services > <access_servicename> Authorization**.

See [Configuring a Session Authorization Policy for Network Access, page 10-31](#), for details.

Step 2 Select **Customize** to customize the authorization policy conditions.

A list of conditions appears. This list includes identity attributes, system conditions, and custom conditions.

See [Customizing a Policy, page 10-4](#), for more information.

Step 3 Select **Use Case** from the **Available** customized conditions and move it to the **Selected** conditions.

Step 4 Select **Authorization Profiles** from the customized results and move it to the **Selected** conditions and click **OK**.

Step 5 In the Authorization Policy Page, click **Create**.

- a. Enter a **Name** for the rule.
- a. In the Conditions area, check **Use Case**, then check whether the value should or should not match.
- a. Select **Host Lookup** and click **OK**.

This attribute selection ensures that while processing the access request, ACS will look for the host and not for an IP address.
- b. Select an **Authorization Profile** from the authorization profiles and move it to the **Selected** results column
- c. Click **OK**.

Step 6 Click **Save Changes**.

Related Topic

- [Managing Access Policies, page 10-1](#)

VPN Remote Network Access

A remote access Virtual Private Network (VPN) allows you to connect securely to a private company network from a public Internet. You could be accessing your company's network from home or elsewhere. The VPN is connected to your company's perimeter network (DMZ). A VPN gateway can manage simultaneous VPN connections.

Related Topics

- [Supported Authentication Protocols, page 4-20](#)
- [Supported Identity Stores, page 4-20](#)
- [Supported VPN Network Access Servers, page 4-21](#)
- [Supported VPN Clients, page 4-21](#)
- [Configuring VPN Remote Access Service, page 4-21](#)

Supported Authentication Protocols

ACS 5.8.1 supports the following protocols for inner authentication inside the VPN tunnel:

- RADIUS/PAP
- RADIUS/CHAP
- RADIUS/MS-CHAPv1
- RADIUS/MS-CHAPv2

With the use of MS-CHAPv1 or MS-CHAPv2 protocols, ACS can generate MPPE keys that is used for encryption of the tunnel that is created.

Related Topics

- [VPN Remote Network Access, page 4-20](#)
- [Supported Identity Stores, page 4-20](#)
- [Supported VPN Network Access Servers, page 4-21](#)
- [Supported VPN Clients, page 4-21](#)
- [Configuring VPN Remote Access Service, page 4-21](#)

Supported Identity Stores

ACS can perform VPN authentication against the following identity stores:

- ACS internal identity store—RADIUS/PAP, RADIUS/CHAP, RADIUS/MS-CHAP-v1, and RADIUS/MS-CHAP-v2
- Active Directory—RADIUS/PAP, RADIUS/MS-CHAP-v1, and RADIUS/MS-CHAP-v2
- LDAP—RADIUS/PAP
- RSA SecurID Server—RADIUS/PAP
- RADIUS Token Server—RADIUS/PAP (dynamic OTP)

Related Topics

- [VPN Remote Network Access, page 4-20](#)
- [Supported Authentication Protocols, page 4-20](#)
- [Supported VPN Network Access Servers, page 4-21](#)
- [Supported VPN Clients, page 4-21](#)
- [Configuring VPN Remote Access Service, page 4-21](#)

Supported VPN Network Access Servers

ACS 5.8.1 supports the following VPN network access servers:

- Cisco ASA 5500 Series
- Cisco VPN 3000 Series

Related Topics

- [VPN Remote Network Access, page 4-20](#)
- [Supported Authentication Protocols, page 4-20](#)
- [Supported Identity Stores, page 4-20](#)
- [Supported VPN Clients, page 4-21](#)
- [Configuring VPN Remote Access Service, page 4-21](#)

Supported VPN Clients

ACS 5.8.1 supports the following VPN clients:

- Cisco VPN Client 5.0 Series
- Cisco Clientless SSL VPN (WEBVPN)
- Cisco AnyConnect VPN client 2.3 Series
- MS VPN client

Related Topics

- [VPN Remote Network Access, page 4-20](#)
- [Supported Authentication Protocols, page 4-20](#)
- [Supported Identity Stores, page 4-20](#)
- [Supported VPN Network Access Servers, page 4-21](#)
- [Configuring VPN Remote Access Service, page 4-21](#)

Configuring VPN Remote Access Service

To configure a VPN remote access service:

- Step 1** Configure the VPN protocols in the Allowed Protocols page of the default network access service. For more information, see [Configuring Access Service Allowed Protocols, page 10-16](#).

- Step 2** Create an authorization profile for VPN by selecting the dictionary type, and the Tunneling-Protocols attribute type and value. For more information, see [Specifying RADIUS Attributes in Authorization Profiles](#), page 9-20.
- Step 3** Click **Submit** to create the VPN authorization profile.

Related Topics

- [VPN Remote Network Access](#), page 4-20
- [Supported Authentication Protocols](#), page 4-20
- [Supported Identity Stores](#), page 4-20
- [Supported VPN Network Access Servers](#), page 4-21
- [Supported VPN Clients](#), page 4-21
- [Configuring VPN Remote Access Service](#), page 4-21

ACS and Cisco Security Group Access

Note ACS requires an additional feature license to enable Security Group Access capabilities.

Cisco Security Group Access, hereafter referred to as Security Group Access, is a new security architecture for Cisco products. You can use Security Group Access to create a trustworthy network fabric that provides confidentiality, message authentication, integrity, and antireplay protection on network traffic.

Security Group Access requires that all network devices have an established identity, and must be authenticated and authorized before they start operating in the network. This precaution prevents the attachment of rogue network devices in a secure network.

Until now, ACS authenticated only users and hosts to grant them access to the network. With Security Group Access, ACS also authenticates devices such as routers and switches by using a name and password. Any device with a Network Interface Card (NIC) must authenticate itself or stay out of the trusted network.

Security is improved and device management is simplified since devices can be identified by their name rather than IP address.

Note The Cisco Catalyst 6500 running Cisco IOS 12.2(33) SXI and DataCenter 3.0 (Nexus 7000) NX-OS 4.0.3 devices support Security Group Access. The Cisco Catalyst 6500 supports Security Group Tags (SGTs); however, it does not support Security Group Access Control Lists (SGACLs) in this release.

To configure ACS for Security Group Access:

- Step 1** Add users.
- This is the general task to add users in ACS and is not specific to Security Group Access. Choose **Users and Identity Stores > Internal Identity Store > Users** and click **Create**. See [Creating Internal Users](#), page 8-13, for more information.
- Step 2** [Adding Devices for Security Group Access](#), page 4-23.
- Step 3** [Creating Security Groups](#), page 4-23.
- Step 4** [Creating SGACLs](#), page 4-24.
- Step 5** [Configuring an NDAC Policy](#), page 4-24.

- Step 6 [Configuring EAP-FAST Settings for Security Group Access, page 4-25.](#)
- Step 7 [Creating an Access Service for Security Group Access, page 4-25.](#)
- Step 8 [Creating an Endpoint Admission Control Policy, page 4-25.](#)
- Step 9 [Creating an Egress Policy, page 4-26.](#)
- Step 10 [Creating a Default Policy, page 4-27.](#)

Adding Devices for Security Group Access

The RADIUS protocol requires a shared secret between the AAA client and the server. In ACS, RADIUS requests are processed only if they arrive from a known AAA client. You must configure the AAA client in ACS with a shared secret.

The Security Group Access device should be configured with the same shared secret. In Security Group Access, every device must be able to act as a AAA client for new devices that join the secured network.

All the Security Group Access devices possess a Protected Access Credential (PAC) as part of the EAP Flexible Authentication via Secured Tunnel (EAP-FAST) protocol. A PAC is used to identify the AAA client. The RADIUS shared secret can be derived from the PAC.

To add a network device:

- Step 1 Choose **Network Resources > Network Devices and AAA Client** and click **Create**. See [Network Devices and AAA Clients, page 7-5](#) for more information.
- Step 2 Choose Fill in the fields in the Network Devices and AAA clients pages:
 - To add a device as a seed Security Group Access device, check **RADIUS** and **Security Group Access**, or to add a device as a Security Group Access client, check **Security Group Access** only.
 - If you add the device as a RADIUS client, enter the **IP Address** and the **RADIUS/Shared Secret**.
 - If you add the device as a Security Group Access device, fill in the fields in the Security Group Access section.
 - You can check **Advanced Settings** to display advanced settings for the Security Group Access device configuration and modify the default settings.

The location or device type can be used as a condition to configure an NDAC policy rule.
- Step 3 Click **Submit**.

Creating Security Groups

Security Group Access uses security groups for tagging packets at ingress to allow filtering later on at Egress. The product of the security group is the security group tag, a 4-byte string ID that is sent to the network device.

The web interface displays the decimal and hexadecimal representation. The SGT is unique. When you edit a security group you can modify the name, however, you cannot modify the SGT ID.

The security group names *Unknown* and *Any* are reserved. The reserved names are used in the Egress policy matrix. The generation ID changes when the Egress policy is modified.

Devices consider only the SGT value; the name and description of a security group are a management convenience and are not conveyed to the devices. Therefore, changing the name or description of the security group does not affect the generation ID of an SGT.

To create a security group:

- Step 1** Choose **Policy Elements > Authorizations and Permissions > Network Access > Security Groups** and click **Create**.
- Step 2** Fill in the fields as described in the [Configuring Security Group Access Control Lists, page 9-32](#).
Note When you edit a security group, the security group tag and the generation ID are visible.
- Step 3** Click **Submit**.

Creating SGACLs

Security Group Access Control Lists (SGACLs) are similar to standard IP-based ACLs, in that you can specify whether to allow or deny communications down to the transport protocol; for example, TCP, User Datagram Protocol (UDP), and the ports; FTP; or Secure Shell Protocol (SSH).

You can create SGACLs that can be applied to communications between security groups. You apply Security Group Access policy administration in ACS by configuring these SGACLs to the intersection of source and destination security groups through a customizable Egress matrix view, or individual source and destination security group pairs.

To create an SGACL:

- Step 1** Choose **Policy Elements > Authorizations and Permissions > Named Permissions Objects > Security Group ACLs**, then click **Create**.
- Step 2** Fill in the fields as described in the [Configuring Security Group Access Control Lists, page 9-32](#).
- Step 3** Click **Submit**.

Configuring an NDAC Policy

The Network Device Admission Control (NDAC) policy defines which security group is sent to the device. When you configure the NDAC policy, you create rules with previously defined conditions, for example, NDGs.

The NDAC policy is a single service, and it contains a single policy with one or more rules. Since the same policy is used for setting responses for authentication, peer authorization, and environment requests, the same SGT is returned for all request types when they apply to the same device.

- Note** You cannot add the NDAC policy as a service in the service selection policy; however, the NDAC policy is automatically applied to Security Group Access devices.

To configure an NDAC policy for a device:

- Step 1** Choose **Access Policies > Security Group Access Control > Security Group Access > Network Device Access > Authorization Policy**.
- Step 2** Click **Customize** to select which conditions to use in the NDAC policy rules.

The Default Rule provides a default rule when no rules match or there are no rules defined. The default security group tag for the Default Rule result is Unknown.

- Step 3** Click **Create** to create a new rule.
- Step 4** Fill in the fields in the NDAC Policy Properties page.
- Step 5** Click **Save Changes**.

Configuring EAP-FAST Settings for Security Group Access

Since RADIUS information is retrieved from the PAC, you must define the amount of time for the EAP-FAST tunnel PAC to live. You can also refresh the time to live for an active PAC.

To configure the EAP-FAST settings for the tunnel PAC:

- Step 1** Choose **Access Policies > Security Group Access Control > > Network Device Access**.
- Step 2** Fill in the fields in the Network Device Access EAP-FAST Settings page.
- Step 3** Click **Submit**.

Creating an Access Service for Security Group Access

You create an access service for endpoint admission control policies for endpoint devices, and then you add the service to the service selection policy.

- Note** The NDAC policy is a service that is automatically applied to Security Group Access devices. You do not need to create an access service for Security Group Access devices.

To create an access service:

- Step 1** Choose **Access Policies > Access Service**, and click **Create**. See [Configuring Access Services, page 10-11](#), for more information.
- Step 2** Fill in the fields in the Access Service Properties—General page as required.
- Step 3** In the Service Structure section, choose **User selected policy structure**.
- Step 4** Select **Network Access**, and check **Identity** and **Authorization**.
- Step 5** Click **Next**.

The Access Services Properties page appears.

- Step 6** In the Authentication Protocols area, check the relevant protocols for your access service.
- Step 7** Click **Finish**.

Creating an Endpoint Admission Control Policy

After you create a service, you configure the endpoint admission control policy. The endpoint admission control policy returns an SGT to the endpoint and an authorization profile. You can create multiple policies and configure the Default Rule policy. The defaults are Deny Access and the Unknown security group.

To add a session authorization policy for an access service:

- Step 1** Choose **Access Policies > Access Services > service > Authorization**.
- Step 2** Configure an Authorization Policy. See [Configuring a Session Authorization Policy for Network Access, page 10-31](#).
- Step 3** Fill in the fields in the Network Access Authorization Rule Properties page.
The Default Rule provides a default rule when no rules match or there are no rules defined. The default for the Default Rule result is Deny Access, which denies access to the network. The security group tag is Unknown.
You can modify the security group when creating the session authorization policy for Security Group Access.
- Step 4** Click **OK**.
- Step 5** Choose **Access Policies > Service Selection Policy** to choose which services to include in the endpoint policy. See [Configuring the Service Selection Policy, page 10-5](#), for more information.
- Step 6** Fill in the fields in the Service Select Policy pages.
- Step 7** Click **Save Changes**.

Creating an Egress Policy

The Egress policy (sometimes called SGACL policy) determines which SGACL to apply at the Egress points of the network based on the source and destination SGT. The Egress policy is represented in a matrix, where the X and Y axis represent the destination and source SGT, respectively, and each cell contains the set of SGACLs to apply at the intersection of these two SGTs.

Any security group can take the role of a source SGT, if an endpoint (or Security Group Access device) that carries this SGT sends the packet. Any security group can take the role of a destination SGT, if the packet is targeting an endpoint (or Security Group Access device) that carries this SGT. Therefore, the Egress matrix lists all of the existing security groups on both axes, making it a Cartesian product of the SGT set with itself (SGT x SGT).

The first row (topmost) of the matrix contains the column headers, which display the destination SGT. The first column (far left) contains the row titles, with the source SG displayed. At the intersection of these axes lies the origin cell (top left) that contains the titles of the axes, namely, Destination and Source.

All other cells are internal matrix cells that contain the defined SGACL. The rows and columns are ordered alphabetically according to the SGT names. Each SGACL can contain 200 ACEs.

Initially, the matrix contains the cell for the unknown source and unknown destination SG. *Unknown* refers to the preconfigured SG, which is not modifiable. When you add an SG, ACS adds a new row and new column to the matrix with empty content for the newly added cell.

To add an Egress policy and populate the Egress matrix:

- Step 1** Choose **Access Policies > Security Group Access Control > Egress Policy**.
The Egress matrix is visible. The security groups appear in the order in which you defined them.
- Step 2** Click on a cell and then click **Edit**.
- Step 3** Fill in the fields as required.
- Step 4** Select the set of SGACLs to apply to the cell and move the selected set to the Selected column.

The ACLS are used at the Egress point of the SGT of the source and destination that match the coordinates of the cell. The SGACLs are applied in the order in which they appear.

- Step 5** Use the Up and Down arrows to change the order. The device applies the policies in the order in which they are configured. The SGACL are applied to packets for the selected security groups.
- Step 6** Click **Submit**.

Creating a Default Policy

After you configure the Egress policies for the source and destination SG in the Egress matrix, Cisco recommends that you configure the Default Egress Policy. The default policy refers to devices that have not been assigned an SGT. The default policy is added by the network devices to the specific policies defined in the cells. The initial setting for the default policy is *Permit All*.

The term *default policy* refers to the ANY security group to ANY security group policy. Security Group Access network devices concatenate the default policy to the end of the specific cell policy.

If the cell is blank, only the default policy is applied. If the cell contains a policy, the resultant policy is the combination of the cell-specific policy which precedes the default policy.

The way the specific cell policy and the default policy are combined depends on the algorithm running on the device. The result is the same as concatenating the two policies.

The packet is analyzed first to see if it matches the ACEs defined by the SGACLs of the cell. If there is no match, the packet falls through to be matched by the ACEs of the default policy.

Combining the cell-specific policy and the default policy is done not by ACS, but by the Security Group Access network device. From the ACS perspective, the cell-specific and the default policy are two separate sets of SGACLs, which are sent to devices in response to two separate policy queries.

To create a default policy:

- Step 1** Choose **Access Policies > Security Group Access Control > Egress Policy** then choose **Default Policy**.
- Step 2** Fill in the fields as in the Default Policy for Egress Policy page.
- Step 3** Click **Submit**.

RADIUS and TACACS+ Proxy Requests

You can use ACS to act as a proxy server having NAS/AAA client in its database, that receives authentication RADIUS requests and authentication and authorization TACACS+ requests from a network access server (NAS) and forwards them to a remote server. ACS then receives the replies for each forwarded request from the remote RADIUS or TACACS+ server and sends them back to the client.

ACS uses the service selection policy to differentiate between incoming authentication and accounting requests that must be handled locally and those that must be forwarded to a remote RADIUS or TACACS+ server.

When ACS receives a proxy request from the NAS, it forwards the request to the first remote RADIUS or TACACS+ server in its list. ACS processes the first valid or invalid response from the remote RADIUS server and does the following:

- If the response is valid for RADIUS, such as Access-Challenge, Access-Accept, or Access-Reject, ACS returns the response back to the NAS.

- If ACS does not receive a response within the specified time period, then after the specified number of retries, or after a specified network timeout, it forwards the request to the next remote RADIUS server in the list.
- If the response is invalid, ACS proxy performs failover to the next remote RADIUS server. When the last failover remote RADIUS server in the list is reached without getting reply, ACS drops the request and does not send any response to the NAS.

ACS processes the first valid or invalid response from the remote TACACS+ server and does the following:

- If the response is valid for TACACS+, such as TAC_PLUS_AUTHEN (REPLY) or TAC_PLUS_AUTHOR (RESPONSE), ACS returns the response back to the NAS.
- If ACS does not receive a response within the specified time period, after the specified number of retries, or after specified network timeout it forwards the request to the next remote TACACS+ server in the list.
- If the response is invalid, ACS proxy performs failover to the next remote TACACS+ server. When the last failover remote TACACS+ server in the list is reached without getting reply, ACS drops the request and does not send any response to the NAS.

You can configure ACS to strip the prefix, suffix, and both from a username (RADIUS) or user (TACACS+). For example, from a username `acme\smith@acme.com`, you can configure ACS to extract only the name of the user, `smith` by specifying `\` and `@` as the prefix and suffix separators respectively.

ACS can perform local accounting, remote accounting, or both. If you choose both, ACS performs local accounting and then moves on to remote accounting. If there are any errors in local accounting, ACS ignores them and moves on to remote accounting.

During proxying, ACS:

- Step 1** Receives the following packets from the NAS and forwards them to the remote RADIUS server:
 - Access-Request
- Step 2** Receives the following packets from the remote RADIUS server and returns them to the NAS:
 - Access-Accept
 - Access-Reject
 - Access-Challenge
- Step 3** Receives the following packets from the NAS and forwards them to the remote TACACS+ server:
 - TAC_PLUS_AUTHOR
 - TAC_PLUS_AUTHEN
- Step 4** Receives the following packets from the remote TACACS+ server and returns them back to the NAS: This behavior is configurable.
 - TAC_PLUS_ACCT

An unresponsive external RADIUS server waits for about *timeout * number of retries* seconds before failover to move to the next server.

There could be several unresponsive servers in the list before the first responsive server is reached. In such cases, each request that is forwarded to a responsive external RADIUS server is delayed for *number of previous unresponsive servers * timeout * number of retries*.

This delay can sometimes be longer than the external RADIUS server timeout between two messages in EAP or RADIUS conversation. In such a situation, the external RADIUS server would drop the request.

You can configure the number of seconds for an unresponsive external TACACS+ server waits before failover to move to the next server.

ACS 5.8.1 supports multiple network interface connectors for RADIUS (IPv4) and TACACS+ (IPv4 and IPv6) proxies. ACS 5.8.1 with Virtual machine, SNS-3495, SNS-3415, or CSACS-1121 platform contains up to four network interfaces and ACS 5.8.1 with SNS-3595 or SNS-3515 supports six network interfaces: Ethernet 0, Ethernet 1, Ethernet 2, Ethernet 3, Ethernet 4, and Ethernet 5. For more information, see [Multiple Network Interface Connector](#) in the Connecting the Network Interface section of *Installation and Upgrade Guide for Cisco Secure Access Control System 5.8.1*.

RADIUS Attribute Rewrite Operation

ACS 5.8.1 supports the RADIUS attribute rewrite operation when ACS is used as a RADIUS proxy server. This feature allows you to manipulate attributes in the RADIUS access requests and responses.

- This feature allows you to add, overwrite, and delete the RADIUS inbound attributes on access requests, which will be redirected from ACS to external servers.
- This feature allows you to add, overwrite, and delete RADIUS outbound attributes on access-accept responses, which will be returned to the client from ACS. The RADIUS attributes update operation on the responses is enabled only for access-accept responses and not for access-reject or challenge responses.

The attribute rewrite operation is configured as part of the Proxy Access Service. This feature is enabled only for RADIUS access requests and not for the accounting requests.

Note ACS 5.8.1 does not allow you to conditionally rewrite RADIUS attribute values.

Example for attribute operation statement:

```
Operator-name ADD new value: "University A"
```

Rewriting RADIUS InBound Requests

You can update the incoming RADIUS requests and rewrite them before sending them to the external server. You can rewrite the attribute values for a specific proxy access service. When this service is selected, ACS performs the operation on the access request and forwards the updated access request to the external server.

The following operations are available in the RADIUS inbound attributes rewrite operation:

- [Adding Attributes to Inbound RADIUS Requests, page 4-29](#)
- [Updating Attributes in Inbound RADIUS Requests, page 4-30](#)
- [Deleting Attributes from Inbound RADIUS Requests, page 4-31](#)

Adding Attributes to Inbound RADIUS Requests

This option is used to add a new attribute value for the selected RADIUS attribute.

- If multiple attributes are not allowed, the add operation adds the new value for the selected attribute only if this attribute does not exist in the request.

Example:

Called-Station-Id – Attribute Multiple NOT allowed:

On the access request:

Called-Station-Id NOT on the request

Attribute operation statement:

Called-Station-Id ADD 1223

Result of the add attribute operation on the request forwarded to the server:

Called-Station-Id =1223

If the Called-Station-Id is on the original request, ACS does not perform the add operation in this example.

- If multiple attributes are allowed, the add operation always adds the attribute with a new value.

Example:

Login-IP-Host – attribute Multiple allowed:

On the access request:

Login-IP-Host=10.56.21.190

Attribute operation statement:

Login-IP-Host ADD 10.56.1.1

Result of the attribute operation on the request forwarded to the server:

Login-IP-Host=10.56.21.190

Login-IP-Host=10.56.1.1

Updating Attributes in Inbound RADIUS Requests

This option is used to update the existing value of a selected RADIUS attribute.

- If multiple attributes are not allowed, the update operation updates the existing attribute with the new value only if the attribute exists on the request.
- If multiple attributes are allowed, the update operation removes all the occurrences of this attribute and adds one attribute with the new value.

Example:

Login-IP-Host – attribute Multiple allowed:

On the access request:

Login-IP-Host=10.56.21.190

Login-IP-Host=10.56.1.1

Attribute operation statement:

Login-IP-Host UPDATE 10.12.12.12

Result of the attribute operation on the request forwarded to the server:

Login-IP-Host=10.12.12.12

- If the attribute is a cisco-avpair (pair of key=value), the update is done according to the key.

Example:

On the access request:

cisco-avpair = url-redirect=www.cisco.com

cisco-avpair = url-redirect=www.yahoo.com

```
cisco-avpair = cmd=show
Attribute operation statement:
cisco-avpair UPDATE new value:[url-redirect=www.google.com]
Result of the attribute operation on the request forwarded to the server:
cisco-avpair = url-redirect=www.google.com
cisco-avpair = cmd=show
```

Deleting Attributes from Inbound RADIUS Requests

This option is used to delete the value of RADIUS inbound attributes.

Example:

Login-IP-Host – attribute Multiple allowed

On the access request:

Login-IP-Host=10.56.21.190

Attribute operation statement:

Login-IP-Host DELETE

Result of the attribute operation on the request forwarded to the server:

Attribute Login-IP-Host is not on the request.

Rewriting RADIUS Outbound Responses

You can update the outgoing RADIUS responses and rewrite them before they are sent to the client devices. You can rewrite the attribute values for a specific proxy access service. When this service is selected, ACS performs the operation on the access accept response and forwards it to the client devices.

The following operations are available in the RADIUS outbound attributes rewrite operation:

- [Adding Attributes to Outbound RADIUS Responses, page 4-31](#)
- [Updating Attributes in Outbound RADIUS Responses, page 4-32](#)
- [Deleting Attributes from OutBound RADIUS Responses, page 4-33](#)

Adding Attributes to Outbound RADIUS Responses

This option is used to add a new attribute value for the selected RADIUS attribute.

- If multiple attributes are not allowed, the add operation adds the new value for the selected attribute only if this attribute does not exist in the access accept response.

Example:

Callback-ID – Attribute Multiple NOT allowed.

On the access accept response from the RADIUS server:

Callback-ID NOT on the access accept response

Attribute operation statement:

Callback-ID ADD 1223

Result of the add attribute operation on the response sent to the client device:

Callback-ID=1223

If the Callback-ID is on the original access accept response, ACS does not perform the add operation in this example.

- If multiple attributes are allowed, the add operation always adds the attribute with a new value.

Example:

Login-IP-Host – attribute Multiple allowed:

On the access accept response from the RADIUS server:

Login-IP-Host=10.58.23.192

Attribute operation statement:

Login-IP-Host ADD 10.58.1.1

Result of the attribute operation on the response sent to the client device:

Login-IP-Host=10.58.23.192

Login-IP-Host=10.58.1.1

Updating Attributes in Outbound RADIUS Responses

This option is used to update the existing value of a selected RADIUS attribute.

- If multiple attributes are not allowed, the update operation updates the existing attributes with a new value only if the attribute exist in the access accept response.
- If multiple attributes are allowed, the update operation removes all the occurrences of this attribute and adds one attribute with a new value.

Example:

Login-IP-Host – attribute Multiple allowed.

On the access accept response from the RADIUS server:

Login-IP-Host=10.58.23.192

Login-IP-Host=10.58.1.1

Attribute operation statement:

Login-IP-Host UPDATE 10.11.11.11

Result of the attribute operation on the response sent to the client device:

Login-IP-Host=10.11.11.11

- If the attribute is cisco-avpair (pair of key=value), the update is done according to the key.

Example:

On the access accept response from the RADIUS server:

cisco-avpair = url-redirect=www.cisco.com

cisco-avpair = url-redirect=www.yahoo.com

cisco-avpair = cmd=show

Attribute operation statement:

cisco-avpair UPDATE new value:[url-redirect=www.google.com]

Result of the attribute operation on the response sent to the client device:

cisco-avpair = url-redirect=www.google.com

cisco-avpair = cmd=show

Deleting Attributes from OutBound RADIUS Responses

This option is used to delete the value of RADIUS outbound attributes.

Example:

Login-IP-Host – attribute Multiple allowed

On the Access Accept Response from the RADIUS server:

Login-IP-Host=10.56.21.190

Attribute Operation statement:

Login-IP-Host DELETE

Result of the attribute operation on the response sent to the client device:

Attribute Login-IP-Host is not in the access accept response.

Related Topics

- [Supported Protocols, page 4-33](#)
- [Supported RADIUS Attributes, page 4-33](#)
- [Configuring Proxy Service, page 4-34](#)

Supported Protocols

The RADIUS proxy feature in ACS supports the following protocols:

- Supports forwarding for all RADIUS protocols
- All EAP protocols
- Protocols not supported by ACS (Since ACS proxy do not interfere into the protocol conversation and just forwards requests)

Note ACS proxy can not support protocols that use encrypted RADIUS attributes.

The TACACS+ proxy feature in ACS supports the following protocols:

- PAP
- ASCII
- CHAP
- MSCHAP authentications types

Related Topics

- [RADIUS and TACACS+ Proxy Requests, page 4-27](#)
- [Supported RADIUS Attributes, page 4-33](#)
- [Configuring Proxy Service, page 4-34](#)

Supported RADIUS Attributes

The following supported RADIUS attributes are encrypted:

- User-Password

- CHAP-Password
- Message-Authenticator
- MPPE-Send-Key and MPPE-Recv-Key
- Tunnel-Password
- LEAP Session Key Cisco AV-Pair

TACACS+ Body Encryption

When ACS receives a packet from NAS with encrypted body (flag TAC_PLUS_UNENCRYPTED_FLAG is 0x0), ACS decrypts the body with common data such as shared secret and sessionID between NAS and ACS and then encrypts the body with common data between ACS and TACACS+ proxy server. If the packet body is in cleartext, ACS will resend it to TACACS+ server in cleartext.

Connection to TACACS+ Server

ACS supports single connection to another TACACS+ server (flag TAC_PLUS_SINGLE_CONNECT_FLAG is 1). If the remote TACACS+ server does not support multiplexing TACACS+ sessions over a single TCP connection ACS will open or close connection for each session.

Related Topics

- [RADIUS and TACACS+ Proxy Requests, page 4-27](#)
- [Supported Protocols, page 4-33](#)
- [Configuring Proxy Service, page 4-34](#)

Configuring Proxy Service

To configure proxy services:

- Step 1** Configure a set of remote RADIUS and TACACS+ servers. For information on how to configure remote servers, see [Creating, Duplicating, and Editing External Proxy Servers, page 7-20](#).
- Step 2** Configure an External proxy service. For information on how to configure a External proxy service, see [Configuring General Access Service Properties, page 10-13](#).
You must select the User Selected Service Type option and choose External proxy as the Access Service Policy Structure in the Access Service Properties - General page.
- Step 3** After you configure the allowed protocols, click **Finish** to complete your External proxy service configuration.

Related Topics

- [RADIUS and TACACS+ Proxy Requests, page 4-27](#)
- [Supported Protocols, page 4-33](#)
- [Supported RADIUS Attributes, page 4-33](#)

FIPS 140-2 Level 1 Implementation

ACS 5.8.1 is compliant with Federal Information Processing Standard (FIPS) 140-2 Level 1. FIPS 140-2 is a United States government computer security standard that is used to accredit cryptographic modules. ACS uses an embedded FIPS 140-2 Level 1 implementation using validated C3M and NSS modules, per the FIPS 140-2 Implementation Guidance section G.5 guidelines.

The FIPS-compliant libraries NSS and Cisco SSL perform a set of self-tests during ACS startup. These two libraries test the integrity of the library files and the algorithms that you use in the cipher suites and certificates. ACS creates log messages to inform the user about the start and end time of the self-tests performed by the FIPS-compliant libraries.

When a self-test fails, a log message is created to inform the user about the failure reason and a resolution for the failure. The specific library is disabled when a library fails a self-test. If the Cisco SSL library fails in a self-test, all AAA and SSH services are disabled and a corresponding message is displayed in logs when you next log in to the ACS web interface. If the NSS library fails in a self-test, all management traffic and the cryptographic information that runs on JAVA are disabled.

In addition, the FIPS standard places limitations on the use of certain algorithms, and to enforce this standard, you must enable FIPS operation in ACS. While in FIPS mode, any attempt to perform functions using a non-FIPS compliant algorithm fails.

By default, FIPS is disabled in upgraded and fresh ACS machines. ACS works in non-FIPS mode by default. To run ACS in FIPS mode, you must enable FIPS mode from the FIPS Global Settings page. When you enable or disable FIPS Mode, runtime services are restarted automatically and the open SSH connections are disconnected in all the nodes of the deployment. When ACS is in FIPS mode, the Secure Shell (SSH) clients uses SSHv2 to access ACS.

FIPS mode supports the following network access authentication protocols:

- EAP-FAST except the anonymous PAC provisioning
- EAP-TLS
- PEAP and its inner methods

FIPS mode does not support the following network access authentication protocols:

- CHAP
- EAP-FAST with anonymous PAC provisioning
- EAP-MD5
- LEAP
- MSCHAPv1
- MSCHAPv2
- PAP

FIPS mode supports the following cipher suites for the management HTTPS server:

- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA

ACS supports different key sizes for certificates: 256, 512, 1024, 2048, and 4096. You cannot enable FIPS mode in ACS when you use CA and server certificates with a key size less than 2048. You must use CA, Certificate Signing Requests (CSRs), and server certificates with a key size greater than or equal to 2048 for ACS to be FIPS-compliant. You may have to get your certificates re-issued if FIPS does not support the encryption (signature or hashes) method used in the certificates.

- Note**
- In FIPS mode, the key size of client certificates less than 1024 bits is not supported
 - ACS supports only the PKCS#8 encrypted certificate private key in FIPS mode.
 - ACS does not support the MD5 and RC4 algorithms in TLS cipher suites, CA certificates, user certificates, and server certificates in FIPS mode.
 - When you register a non-FIPS node in a FIPS enabled deployment, the non FIPS node's server certificates, CA certificates, and CSRs are validated for FIPS compliance.
 - When you register a FIPS enabled node in a deployment where FIPS is not enabled, the primary ACS instance's server certificate is validated by the secondary node for FIPS compliance if the trusted management communication is enabled.

When you try to turn on FIPS mode in ACS, if ACS detects at least one protocol or certificate that is not supported by the FIPS 140-2 Level 1 standard, ACS displays a warning with a list of prerequisites that must be met, and FIPS mode is not enabled until the issues are resolved.

- Tip** Cisco recommends that you do not enable FIPS mode before completing any database migration process.

Before You Begin

- The key size of CA certificates, CSRs, and server certificates that are used in ACS should be greater than or equal to 2048 bits.
- Make sure that PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-MD5, LEAP, and Anonymous PAC Provisioning in EAP-FAST protocols are disabled.
- Make sure that the remote log target type is set as **Secure TCP Syslog** in the **System Administration > Configuration > Log Configuration > Remote Log Targets > Create** page.
- Make sure that the checkbox **Accept any Syslog server** in the **System Administration > Configuration > Log Configuration > Remote Log Targets > Create** page is unchecked.
- Make sure that the checkbox **Use Secure Authentication** in the **Users and Identity Stores > External Identity Stores > LDAP > Server Connection** page is checked.

To enable FIPS mode:

- Step 1** Choose **System Administration > Configuration > Global System Options > FIPS Global Settings**.

The FIPS Global Settings page appears.

- Step 2** Check the **Enable FIPS** check box.

- Step 3** Click **Submit**.

The following message is displayed in a popup window:

This operation disconnects all open SSH connections and restarts the runtime services of all ACS instances in a deployment. Do you wish to continue?

- Step 4** Click **OK**.

To disable FIPS mode:

- Step 1** Choose **System Administration > Configuration > Global System Options > FIPS Global Settings**.

The FIPS Global Settings page appears.

- Step 2** Uncheck the **Enable FIPS** check box.

- Step 3** Click **Submit**.

The following message is displayed in a popup window:

This operation disconnects all open SSH connections and restarts the runtime services of all ACS instances in a deployment. Do you wish to continue?

Step 4 Click **OK**.

Related Topics

- [Cisco NAC Agent Requirements When FIPS Mode Is Enabled, page 4-37](#)

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 ACS network. (These TLS 1.0 settings should be enabled in Internet Explorer.) Therefore, client machines must have Windows Internet Explorer installed and must have TLS1.0 enabled to allow for ACS posture assessment functions to operate on client machines that access the network. The ACS Agent can automatically enable the TLS 1.0 setting in Windows Internet Explorer if FIPS mode has been enabled in ACS.

Enabling and Disabling IPv6 for Network Interfaces

ACS 5.8.1 provides the capability to disable the IPv6 stack for all interfaces or for a specific interface. By default, IPv6 is enabled for all interfaces.

You can enable or disable the IPv6 stack from the ACS CLI in configuration mode. You should restart the ACS services to reflect correct IPv6 behavior even though the CLI prompts for a confirmation.

When you disable IPv6 at the global level, you cannot enable it at the interface level.

Even when you disable IPv6, ACS allows IPv6 static address configuration, which is shown in the running configuration. However, it will not be used.

For more information on the **ipv6 enable** command and its usage, see the [CLI Reference Guide for Cisco Secure Access Control System 5.8.1](#).



Understanding My Workspace

The Cisco Secure ACS web interface is designed to be viewed using Microsoft Internet Explorer and Mozilla Firefox browsers. For more information on supported browser versions, see [Release Notes for Cisco Secure Access Control System 5.8.1](#). The web interface not only makes viewing and administering ACS possible, but it also allows you to monitor and report on any event in the network.

These reports track connection activity, show which users are currently logged in, list the failed authentication and authorization attempts, and so on.

The My Workspace drawer contains:

- [Welcome Page, page 5-1](#)
- [Task Guides, page 5-2](#)
- [My Account Page, page 5-2](#)
- [Login Banner, page 5-3](#)
- [Using the Web Interface, page 5-4](#)
- [Importing and Exporting ACS Objects Through the Web Interface, page 5-19](#)
- [Common Errors, page 5-25](#)
- [Accessibility, page 5-28](#)

Welcome Page

The Welcome page appears when you start ACS, and it provides shortcuts to common ACS tasks and links to information.

You can return to the Welcome page at any time during your ACS session. To return to this page, choose **My Workspace > Welcome**.

Table 5-1 *Welcome Page*

Field	Description
Before You Begin	Contains a link to a section that describes the ACS policy model and associated terminology.
Getting Started	Links in this section launch the ACS Task Guides, which provide step-by-step instructions on how to accomplish ACS tasks.
Quick Start	Opens the Task Guide for the Quick Start scenario. These steps guide you through a minimal system setup to get ACS going quickly in a lab, evaluation, or demonstration environment.

Table 5-1 Welcome Page (continued)

Field	Description
Initial System Setup	Opens the Task Guide for initial system setup. This scenario guides you through the steps that are required to set up ACS for operation as needed; many steps are optional.
Policy Setup Steps	Opens the Task Guide for policy setup. This scenario guides you through the steps that are required to set up ACS policies.
New in ACS 5	Options in this section link to topics in the ACS online help. Click an option to open the online help window, which displays information for the selected topic. Use the links in the online help topics and in the Contents pane of the online help to view more information about ACS features and tasks.
Tutorials & Other Resources	Provides links to: <ul style="list-style-type: none"> • Introduction Overview video. • Configuration guide that provides step-by-step instructions for common ACS scenarios.

In ACS 5.8.1, you can also see a banner in the welcome page. You can customize this **After Login** banner text from the Login Banner page.

Task Guides

From the My Workspace drawer, you can access Tasks Guides. When you click any of the tasks, a frame opens on the right side of the web interface. This frame contains step-by-step instructions, as well as links to additional information. ACS provides the following task guides:

- Quick Start—Lists the minimal steps that are required to get ACS up and running quickly.
- Initial System Setup—Lists the required steps to set up ACS for basic operations, including information about optional steps.
- Policy Setup Steps—Lists the required steps to define ACS access control policies.

My Account Page



Note

Every ACS administrator account is assigned one or more administrative roles. Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in certain procedures. See [Configuring System Administrators and Accounts, page 16-3](#) to configure the appropriate administrator privileges.

Use the My Account page to update and change the administrator password for the administrator that is currently logged in to ACS.

To display this page, choose **My Workspace > My Account**.

Table 5-2 My Account Page

Field	Description
General	Read-only fields that display information about the currently logged-in administrator: <ul style="list-style-type: none"> Administrator name Description E-mail address, if it is available
Change Password	Displays rules for password definition according to the password policy. To change your password: <ol style="list-style-type: none"> In the Password field, enter your current password. In the New Password field, enter a new password. In the Confirm Password field, enter your new password again.
Assigned Roles	Displays the roles that are assigned to the currently logged-in administrator.

Related Topics

- [Configuring Authentication Settings for Administrators, page 16-14](#)
- [Changing the Administrator Password, page 16-30](#)

Login Banner

ACS 5.8.1 supports customizing of the login banner texts. You can set two sets of banner text; for instance, before logging you can display one banner text, and after logging in you can display another banner text. You can do this customization from the Login Banner page. The copyright statement is default for both the banners. ACS 5.8.1 displays the role of ACS in the login banners. The role can be primary, primary log collector, secondary, or secondary log collector.

You can also configure login banners for ACS CLI. To display a banner text before and after logging in to ACS CLI, use the **banner** command in the EXEC mode. The banners that are configured using the **banner** command from ACS CLI do not reflect in ACS web interface, whereas the banners that are configured in ACS web interface impacts the ACS CLI banner. For more information on banner command, see the [CLI Reference Guide for Cisco Secure Access Control System](#).

**Note**

ACS does not support ' and " symbols in login banner text.

To customize the login banner, choose **My Workspace > Login Banner**.

Table 5-3 Login Banner Page

Field	Description
Before Login	Enter the text that you want to display in the banner before login.
After Login	Enter the text that you want to display in the banner after login.

Using the Web Interface

You can configure and administer ACS through the ACS web interface, in which you can access pages, perform configuration tasks, and view interface configuration errors. This section describes:

- [Accessing the Web Interface, page 5-4](#)
- [Understanding the Web Interface, page 5-6](#)
- [Common Errors, page 5-25](#)
- [Accessibility, page 5-28](#)

Accessing the Web Interface

The ACS web interface is supported on HTTPS-enabled Microsoft Internet Explorer and Mozilla Firefox browsers. For more information on supported browser versions, see [Release Notes for Cisco Secure Access Control System 5.8.1](#).

This section contains:

- [Logging In, page 5-4](#)
- [Logging Out, page 5-5](#)

Logging In

To log in to the ACS web interface for the first time after installation:

- Step 1** Enter the ACS URL in your browser, for example, **`https://acs_host/acsadmin`**, **`https://[IPv6 address]/acsadmin`**, or **`https://ipv4 address/acsadmin`**, where `/acs_host` is the IP address or Domain Name System (DNS) hostname. The DNS hostname works for IPv6 when the given IP address is resolvable to both IPv4 and IPv6 formats.



Note Launching the ACS web interface using IPv6 addresses is not supported in Mozilla Firefox versions 4.x or later.

The login page appears.

- Step 2** Enter **ACSAdmin** in the Username field; the value is not case-sensitive.
- Step 3** Enter **default** in the Password field; the value is case-sensitive.
- This password (default) is valid only when you log in for the first time after installation. Click **Reset** to clear the Username and Password fields and start over, if needed.
- Step 4** Click **Login** or press **Enter**.
- The login page reappears, prompting you to change your password.
- ACS prompts you to change your password the first time you log in to the web interface after installation and in other situations based on the authentication settings that is configured in ACS.
- Step 5** Enter **default** in the Old Password field, and enter a new password in the New Password and the Confirm Password fields.
- If you forget your password, use the **acs reset-password** command to reset your password to default. See the *CLI Reference Guide for Cisco Secure Access Control System, 5.8.1* for more information.

Step 6 Click **Login** or press **Enter**.

You are prompted to install a valid license:



Note The license page only appears the first time that you log in to ACS.

Step 7 See [Installing a License File, page 18-39](#) to install a valid license.

- If your login is successful, the main page of the ACS web interface appears.
- If your login is unsuccessful, the following error message appears:

Access Denied. Please contact your Security Administrator for assistance.

The Username and Password fields are cleared.

Step 8 Re-enter the valid username and password, and click **Login**.



Note When you use Internet Explorer to view the ACS web interface, if the Enhanced Security Configuration (ESC) is enabled, you would observe issues in displaying pages and pop-ups of the ACS web interface. To overcome this issue, you must disable the ESC from the Internet Explorer settings.



Note The latest Internet Explorer and Mozilla Firefox browser versions do not allow the self-signed certificates of key size less than 1024 to provide enhanced network security. Due to this restriction, you must generate and use a self-signed certificate of key size greater than or equal to 1024 to access the ACS web interface in the latest Internet Explorer and Mozilla Firefox browser versions.

Logging Out

Click **Logout** in the ACS web interface header to end your administrative session. A dialog box appears asking if you are sure you want to log out of ACS. Click **OK**.

**Caution**

For security reasons, Cisco recommends that you log out of the ACS when you complete your administrative session. If you do not log out, the ACS web interface logs you out if your session remains inactive for a configurable period of time, and does not save any unsubmitted configuration data. See [Configuring Session Idle Timeout, page 16-17](#) for configuring session idle timeout.

Understanding the Web Interface

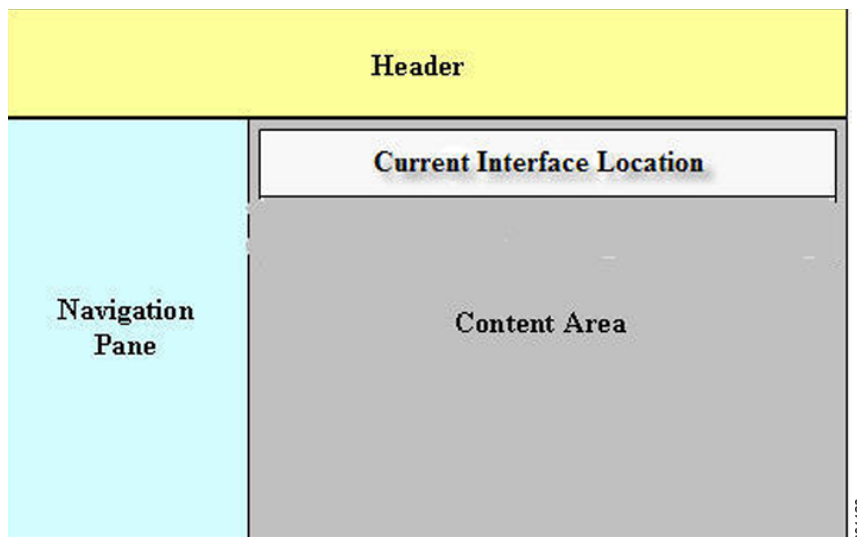
The following sections explain the ACS web interface:

- [Web Interface Design, page 5-6](#)
- [Header, page 5-6](#)
- [Navigation Pane, page 5-7](#)
- [Content Area, page 5-9](#)

Web Interface Design

[Figure 5-1](#) shows the overall design of the ACS web interface.

Figure 5-1 ACS Web Interface



The interface contains:

- [Header, page 5-6](#)
- [Navigation Pane, page 5-7](#)
- [Content Area, page 5-9](#)

Header

Use the header to:

- Identify the current user (your username)

- Access the online help
- Log out
- Access the About information, where you can find information about which ACS web interface version is installed.

These items appear on the right side of the header (see [Figure 5-2](#)).

Figure 5-2 Header



Related Topics

- [Navigation Pane, page 5-7](#)
- [Content Area, page 5-9](#)

Navigation Pane

Use the navigation pane to navigate through the drawers of the web interface (see [Figure 5-3](#)).

Figure 5-3 Navigation Pane



[Table 5-4](#) describes the function of each drawer.

Table 5-4 Navigation Pane Drawers

Drawer	Function
My Workspace	Access the Task Guide and Welcome page with shortcuts to common tasks and links to more information. See Understanding My Workspace, page 5-1 for more information.
Network Resources	Configure network devices, AAA clients, and network device groups. See Managing Network Resources, page 7-1 for more information.
Users and Identity Stores	Configure internal users and identity stores. See Managing Users and Identity Stores, page 8-1 for more information.

Table 5-4 *Navigation Pane Drawers*

Drawer	Function
Policy Elements	Configure policy conditions and results. See Managing Policy Elements, page 9-1 for more information.
Access Policies	Configure access policies. See Managing Access Policies, page 10-1 for more information.
Monitoring and Reports	View log messages. See Monitoring and Reporting in ACS, page 11-1 for more information.
System Administration	Administer and maintain your ACS. See Managing System Administrators, page 16-1 for more information.

To open a drawer, click it. A list of options for that drawer appears. You can view the contents of only one drawer at a time. When you open a drawer, any previously open drawer automatically closes.

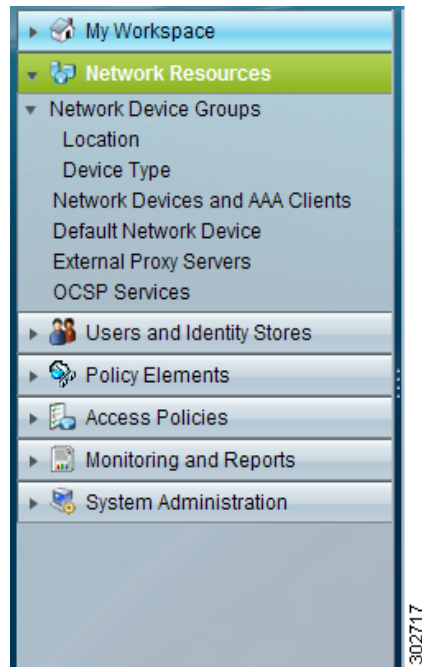
Click an option to view the hierarchy of items and the current configuration, and perform configuration tasks associated with that option in the content area. See [Content Area, page 5-9](#) for more information about the content area.

To hide the navigation pane and expand the content area, click the collapse arrow, which is centered vertically between the navigation pane and content area. Click the collapse arrow again to reveal the navigation pane.

The options listed beneath drawers in the navigation pane are organized in a tree structure, where appropriate. The options in the tree structure are dynamic and can change based on administrator actions. Creating, deleting, or renaming objects in the content area can change the option display in the navigation pane.

For example, beneath the **Network Resources > Network Device Groups** option, there are two preconfigured network device groups (options)—Location and Device Type.

[Figure 5-4](#) shows that the administrator has used the Network Device Groups option page to create an additional network device group called Business, which appears in the tree structure in the navigation pane.

Figure 5-4 Navigation Pane—Dynamic Tree Structure**Related Topics**

- [Header, page 5-6](#)
- [Content Area, page 5-9](#)

Content Area

Use the content area to view your current location in the interface, view your configuration, configure AAA services, and administer your ACS.

The content area can contain:

- [Web Interface Location, page 5-9](#)
- [List Pages, page 5-10](#)
- [Secondary Windows, page 5-14](#)
- [Rule Table Pages, page 5-17](#)

Web Interface Location

Your current location in the interface appears at the top of the content area. [Figure 5-5](#) shows that the location is the Policy Elements drawer and the Network Devices and AAA Clients page.

Using this location as an example, ACS documentation uses this convention to indicate interface locations—**Policy Elements > Policy Conditions > Network Devices and AAA Clients > Location**. The remainder of the content area shows the content of the chosen page.

The interface location also displays the action that you are configuring. For example, if you are in the **Users and Identity Stores > Internal Identity Stores > Users** page and you attempt to duplicate a specific user, the interface location is stated as:

Users and Identity Stores > Internal Identity Stores > Users > Duplicate: *user_name*, where *user_name* is the name of the user you chose to duplicate. ACS documentation also uses this convention.

List Pages

List pages contain a list of items (see [Figure 5-5](#)).
 You can use list pages to delete one or more items from an option that you chose in the navigation pane.

Figure 5-5 List Page

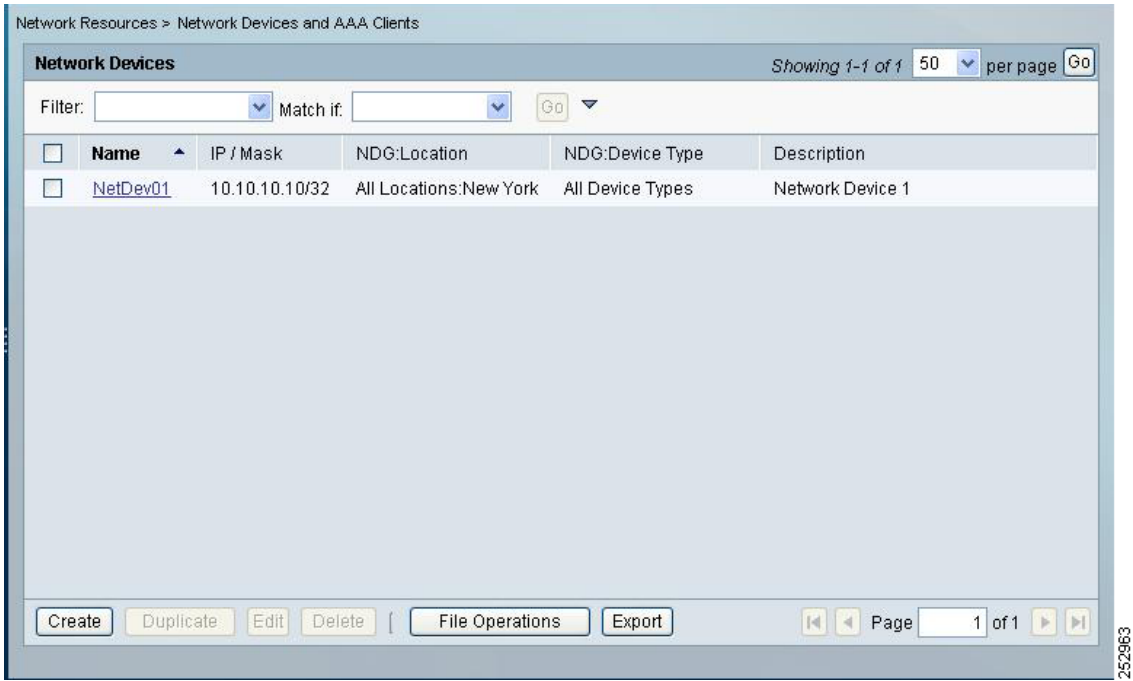


Table 5-5 describes the content area buttons and fields that list pages have in common.

Table 5-5 Common Content Area Buttons and Fields for List Pages

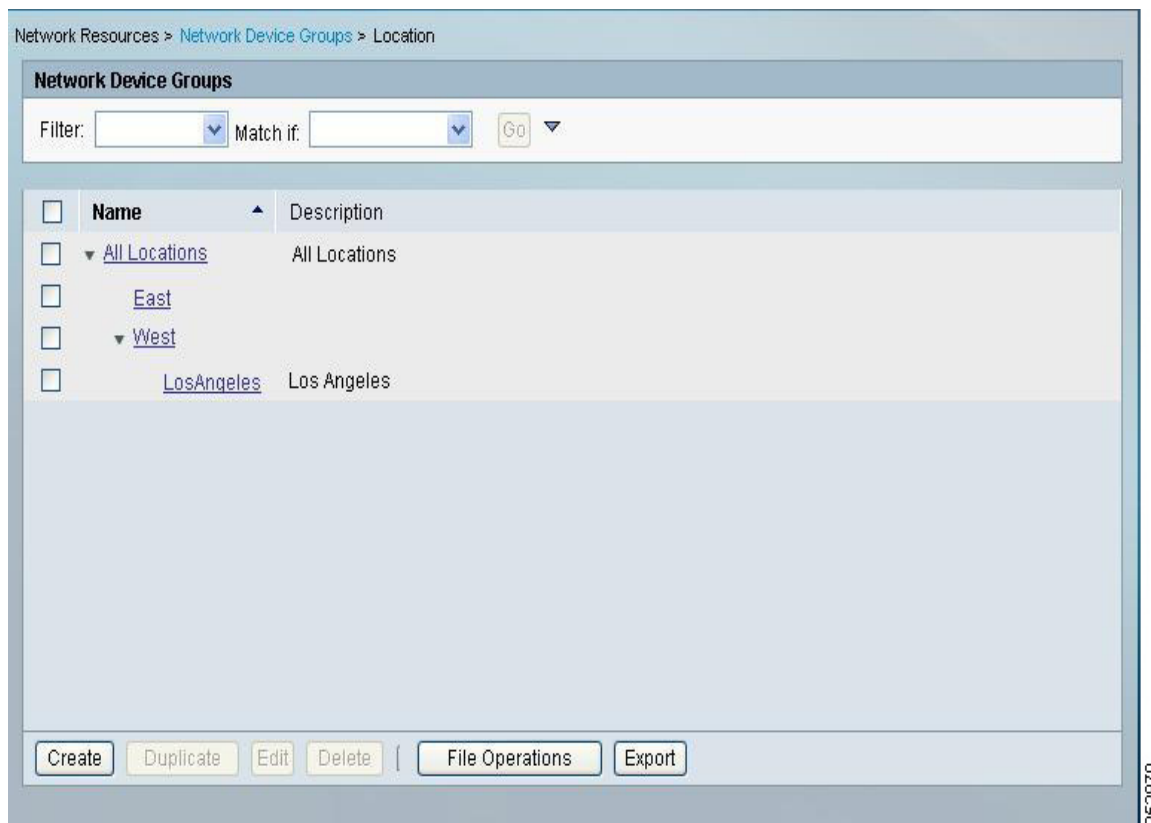
Button or Field	Description
Rows per page	Use the drop-down list to specify the number of items to display on this page. Options: <ul style="list-style-type: none"> 10—Up to 10. 25—Up to 25. 50—Up to 50. 100—Up to 100.
Go	Click to display the number of items you specify in the Rows per page field.
Check box or radio button	Chooses or does not choose items in a list, for edit, duplicate, or delete actions. Options: <ul style="list-style-type: none"> Check (a check box) or click (a radio button)—Chooses an item. Check the check box in the header row to choose all items in the list. Check the individual check boxes to choose specific items in the list. Uncheck (a check box) or unclick (a radio button)—Does not choose an item.

Table 5-5 Common Content Area Buttons and Fields for List Pages

Button or Field	Description
List column	A tabular or hierarchical view of items associated with a specific configuration task. Figure 5-5 shows the list column as a list of configured network device names; the heading of this list column is Name.
Scroll bar	Use the content area scroll bar to view all the data in a page, if needed.
Create	Click to create a new item. A wizard or single page appears in the content area. When you click Create , any selections that you made in the content area are ignored and the content area displays an Edit page with page-specific default values, if any.
Duplicate	Click to duplicate a selected item. A single page or a tabbed page appears in the content area.
Edit	Click to edit a selected item. A single page or a tabbed page appears in the content area.
Delete	Click to delete one or more selected items. A dialog box that queries <i>Are you sure you want to delete item/items?</i> appears for the item, or items, you chose to delete. The confirmation dialog box contains OK and Cancel. Click: <ul style="list-style-type: none"> OK—Deletes the selected item or items. The list page appears without the deleted item. Cancel—Cancels the delete operation. The list page appears with no changes. <p>You can only delete items that you can view on a page, including the content of a page that you can view by using the scroll bar.</p> <p>For tables that span more than one page, your selections of rows to delete for pages that you cannot view are ignored and those selections are not deleted.</p>
Page <i>num</i> of <i>n</i>	Enter the number of the page you want to display in the content area of the list page, where <i>num</i> is the page you want to display, then click Go . Not available for tree table pages.
Direction arrows	Click the arrows on the lower right side of the content area to access the first page, previous page, next page, or last page. The arrows are active when required. Not available for tree table pages.

Tree table pages are a variation of list pages (see [Figure 5-6](#)). You can perform the same operations on tree table pages that you can on list pages, except for paging. In addition, with tree table pages:

- A darker background color in a row indicates the top level of a tree.
- If the first folder of a tree contains fewer than 50 items, the first folder is expanded and all others are collapsed. You must use the expanding icon (+) to view the contents of the collapsed folders.
- If the first folder of a tree contains 50 or more items, all folders in the tree are collapsed. You must click the expanding icon (+) to view the contents of the folders.
- If you check the check box for a folder (a parent), it chooses all children of that folder.
- If you check the check box of a folder (a parent), and then uncheck any of the children, the parent folder is unchecked automatically.

Figure 5-6 *Tree Table Page***Filtering**

Large lists in a content area window or a secondary window (see [Figure 5-9](#)) can be difficult to navigate through and select the data that you want. You can use the web interface to filter data in these windows to reduce the data that appears in a list, based on criteria and conditions that you choose. [Table 5-6](#) describes the filtering options.

**Note**

Not all filtering options are available in all fields.

Table 5-6 *Filtering in the Content Area Window and Secondary Windows*

Button or Field	Description
Filter (drop-down list box)	Select the name of the column from the drop-down list box on which to filter.
Match if (drop-down list box)	<p>Select the condition you want to apply to your filter action:</p> <ul style="list-style-type: none"> • Contains • Doesn't Contain • Ends With • Equals • Is Empty • Not Empty • Not Equals • Starts With <p>The condition is applied to the column you select in the Filter drop-down list box.</p>
v (down arrow)	Click to add an additional filter row on which to choose conditions to narrow or expand your filter action. The text <i>And:</i> precedes the additional filter row.
^ (up arrow)	Click to remove an extraneous filter row.
Go	Click to execute your filter action.
Clear Filter	Click to clear any current filter options.
OK	<p>Click to add the selected data to your configuration and close the secondary window.</p> <p>This button is only available in secondary windows (see Figure 5-9).</p>

**Note**

For tree table pages, you can only perform filtering on a root node, the top-most parent.

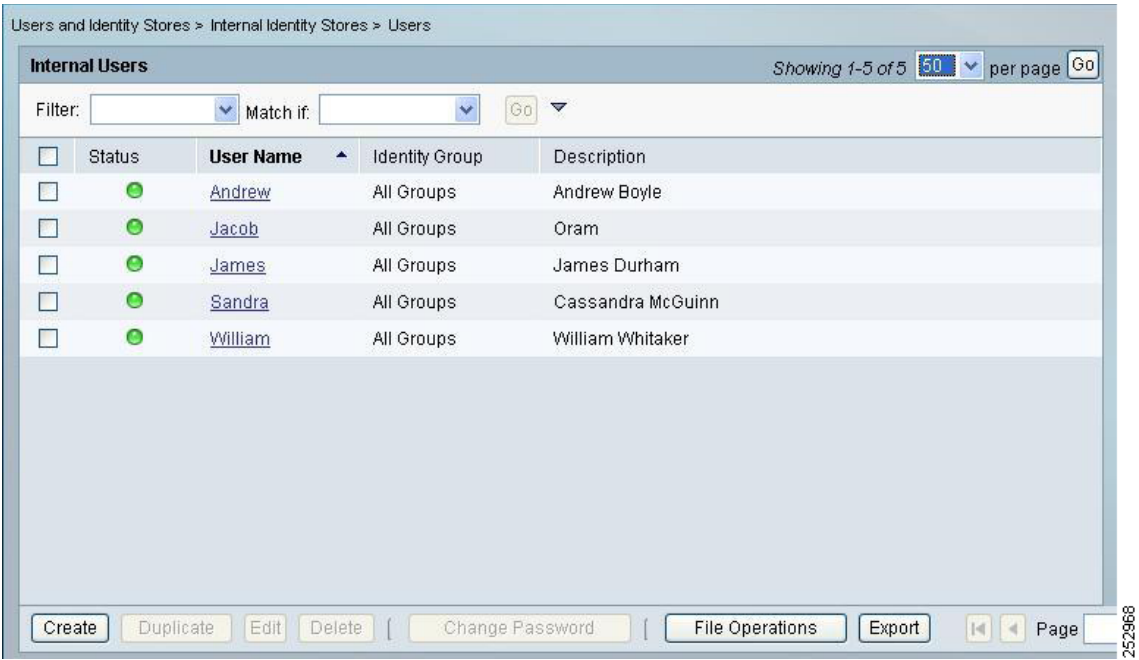
Sorting

Most nontree list pages support sorting by the Name column or the Description column, when available. You can sort pages in an ascending or descending manner.

For pages that do not have a Name or Description column, the sorting mechanism may be supported in the left-most column of the page, or the Description column. Place your cursor over a column heading to determine if sorting is available for a column. If sorting is available, the cursor turns into a hand and the text *Click to sort* appears.

When a table is sorted, the column heading text darkens and an up arrow or down arrow appears the text (see [Figure 5-7](#)). Click the arrow to resort in the opposing manner.

Figure 5-7 *Sorting Example*



Secondary Windows

The content area serves as the launching place for any secondary (popup) windows that you access by clicking Select (see Figure 5-8) from single, tabbed, or wizard pages. You use these secondary windows to filter and select data that you want to use in your configuration (see Figure 5-9 and Table 5-6).

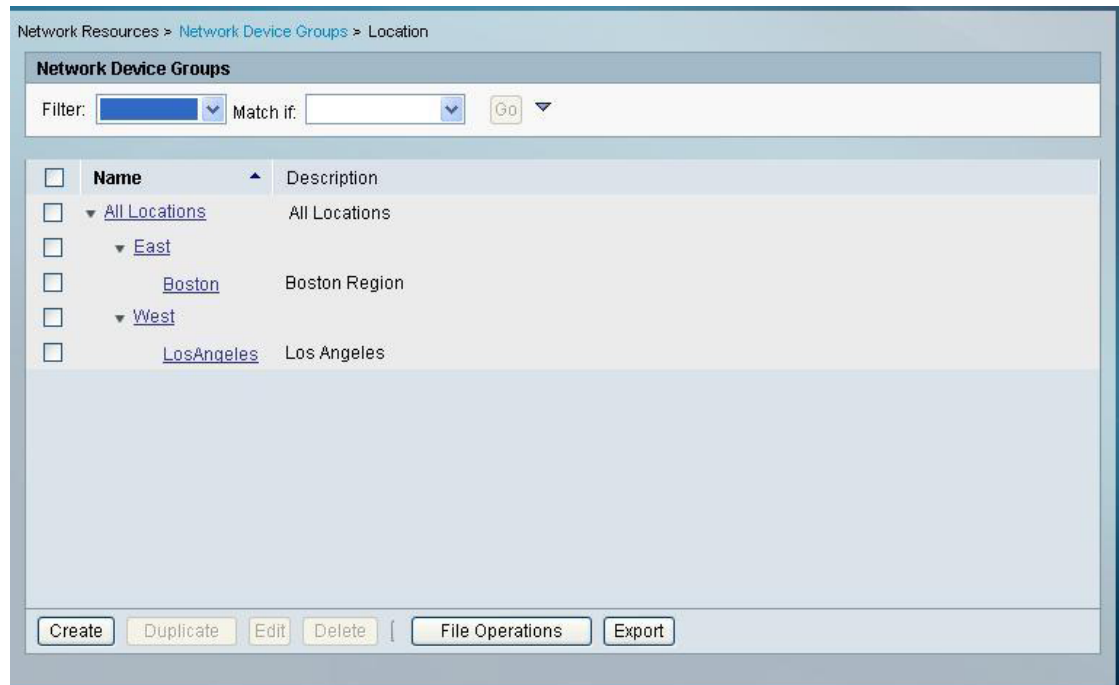
You can select one or more items from a secondary window to include in your configuration, dependent upon the selection option.

Items listed in a secondary window with radio buttons allow you to select one item to include in your configuration and items listed with check boxes allow you to select multiple items.

Figure 5-8 Select Button—Accesses Secondary Windows



Figure 5-9 Secondary Window



In addition to selecting and filtering data, you can create a selectable object within a secondary window.

For example, if you attempt to create a users internal identity store, and click **Select** to assign the store to an identity group (a selectable object), but the identity group you want to associate it with is not available for selection, you can click **Create** within the secondary window to create the object you want.

After you have created the object and clicked **Submit**, the secondary window is refreshed with the newly created object, which you can then select for your configuration. In this example, you can select the newly created identity group to assign it to the users internal identity store.

Transfer Boxes

Transfer boxes are a common element in content area pages (see [Figure 5-10](#)). You use these boxes to select and remove items for use in your configuration and order them according to your needs.

[Figure 5-10](#) shows the transfer box options. [Table 5-7](#) describes the transfer box options.

Figure 5-10 Transfer Box

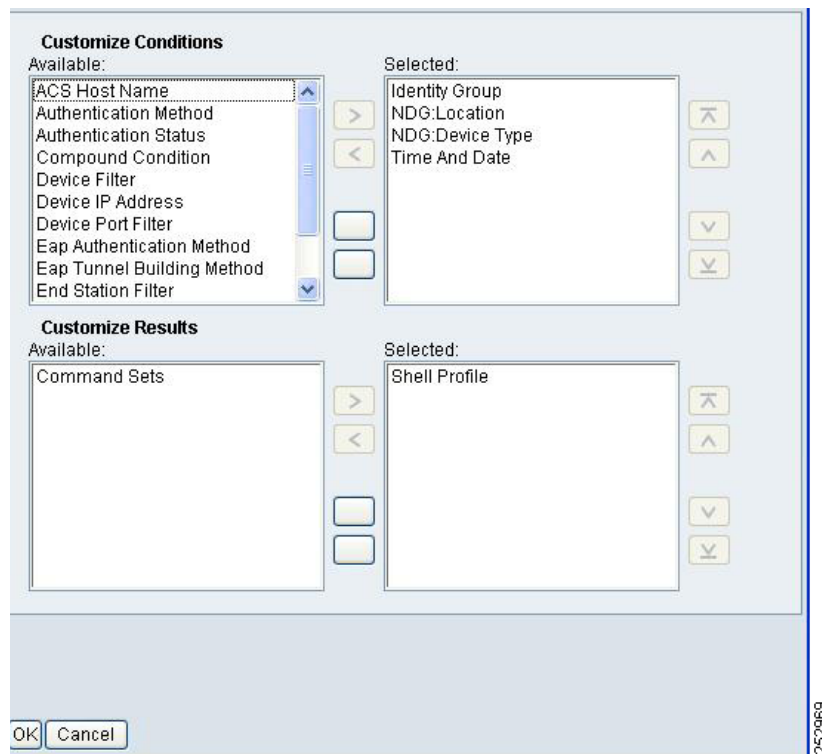


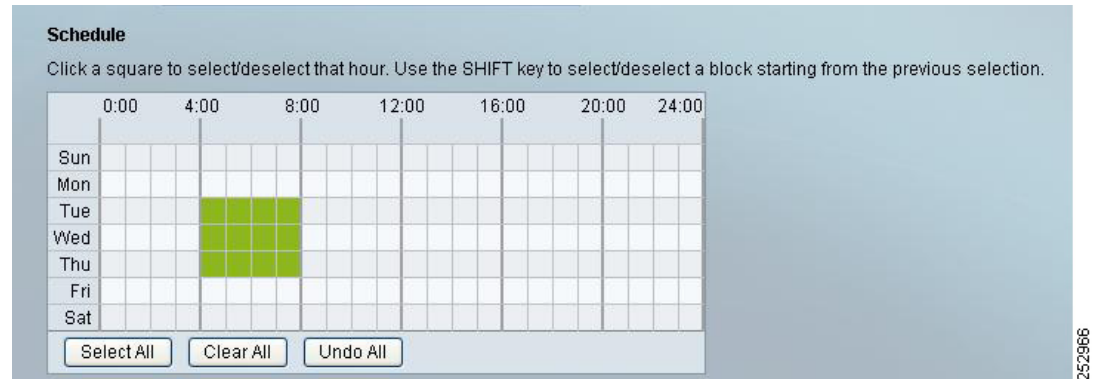
Table 5-7 *Transfer Box Fields and Buttons*

Field or Button	Description
Available	List of available items for selection.
Selected	Ordered list of selected items.
Right arrow (>)	Click to move one selected item from the Available list to the Selected list.
Left arrow (<)	Click to move one selected item from the Selected list to the Available list.
Double right arrow (>>)	Click to move all items from the Available list to the Selected list.
Double left arrow (<<)	Click to move all items from the Selected list to the Available list.
Up arrow with above score	Click to move one selected item to the top of the ordered Selected items list.
Up arrow	Click to move one selected item up one position in the ordered Selected items list.
Down arrow	Click to move one selected item down one position in the ordered Selected items list.
Down arrow with underscore	Click to move one selected item to the bottom of the ordered Selected items list.

Schedule Boxes

Schedule boxes are a common element in content area pages (see [Table 5-6](#)). You use them to select active times for a policy element from a grid, where each row represents a day of the week and each square in a row represents an hour in a day.

Click one square to make one hour active. [Table 5-8](#) describes the Schedule box options.

Figure 5-11 *Schedule Box***Table 5-8** *Schedule Box Fields and Buttons*

Field or Button	Description
Mon	Row that indicates Monday of every week of every year.
Tue	Row that indicates Tuesday of every week of every year.
Wed	Row that indicates Wednesday of every week of every year.
Thu	Row that indicates Thursday of every week of every year.
Fri	Row that indicates Friday of every week of every year.
Sat	Row that indicates Saturday of every week of every year.
Sun	Row that indicates Sunday of every week of every year.
0:00 to 24:00	Indicates the hours of a day in columns, where 0:00 = the hour that begins the second after midnight Eastern Standard Time (EST), and 24:00 = midnight to 1:00 a.m., in the time zone in which your ACS instance is located.
Square (of the grid)	Click one square to make one hour active.
Set All	Click to select all squares (hours).
Clear All	Click to deselect all squares (hours).
Undo All	Click to remove your most recent selections.

Rule Table Pages

Rule table pages display the rules that comprise policies. You can reorder rules within a rule table page and submit the policy that is associated with a table. You can access properties and customization pages from rule tables to configure your policies.

For more information on specific rule table pages, and properties and customization pages, see [Managing Access Policies, page 10-1](#).

Directly above the rule table are two display options:

- Standard Policy—Click to display the standard policy rule table.
- Exception Policy—Click to display the exception policy rule table, which takes precedence over the standard policy rule table content.

[Table 5-9](#) describe the common options of standard and exception rule table pages:

Table 5-9 Rule Table Page Options

Option	Description
#	<p>Ordered column of rules within the rule table. You can renumber the rules by reordering, adding, or deleting rules and then clicking Save Changes to complete the renumbering.</p> <p>New rules are added to the end of the ordered column, so you must reorder them if you want to move a new rule to a different position within the ordered list.</p> <p>You cannot reorder the default (catch-all) rule, which remains at the bottom of the rule table.</p>
Check box	Click one or more check boxes to select associated rules on which to perform actions.
Status	<p>(<i>Display only.</i>) Indicates the status of rules within the rule table. The status can be:</p> <ul style="list-style-type: none"> Enabled—Indicated by a green (or light colored) circle with a white check mark. Disabled—Indicated by a red (or dark colored circle) with a white x. Monitor-only—Indicated by a gray circle with a black i.
Name	<p>Unique name for each rule (except the default, catch-all rule). Click a name to edit the associated rule. When you add a new rule, it is given a name in the format <code>Rule-num</code>, where <i>num</i> is the next available consecutive integer.</p> <p>You can edit the name to make it more descriptive. Cisco recommends that you name rules with concatenation of the rule name and the service and policy names.</p>
Conditions	Variable number of condition types are listed, possibly in subcolumns, dependent upon the policy type.
Results	Variable number of result types are listed, possibly in subcolumns, dependent upon the policy type.
Hit Counts column	View the hits counts for rules, where hits indicate which policy rules are invoked.
Rules scroll bar	Use the scroll bar at the right of the rules rows to scroll up and down the rules list.
Conditions and results scroll bar	Use the scroll bar beneath the Conditions and Results columns to scroll left and right through the conditions and results information.
Default rule	Click to configure the catch-all rule. This option is not available for exception policy rule tables.
Customize	Click to open a secondary window where you can determine the set and order of conditions and results used by the rule table.
Hit Counts button	<p>Click to open a secondary window where you can:</p> <ul style="list-style-type: none"> View when the hit counters were last reset or refreshed. View the collection period. Request a reset or refresh of the hit counts. <p>See Displaying Hit Counts, page 10-10 for more information.</p>
Move to...	Use the ^ and v buttons to reorder selected rules within the rule table.
Save Changes	Click to submit your configuration changes.
Discard Changes	Click to discard your configuration changes prior to saving them.

Related Topic

- [ACS 5.x Policy Model, page 3-1](#)

Importing and Exporting ACS Objects Through the Web Interface

You can use the import functionality in ACS to add, update, or delete multiple ACS objects at the same time. ACS uses a comma-separated values (CSV) file to perform these bulk operations. This .csv file is called an import file. ACS provides a separate .csv template for add, update, and delete operations for each ACS object.

The first record in the .csv file is the header record from the template that contains column (field) names. You must download these templates from the ACS web interface. The header record from the template must be included in the first row of any .csv file that you import.

**Note**

Note: You cannot use the same template to import all the ACS objects. You must download the template that is designed for each ACS object and use the corresponding template while importing the objects. However, you can use the export file of a particular object, retain the header and update the data, and use it as the import file of the same object.

You can use the export functionality to create a .csv file that contains all the records of a particular object type that are available in the ACS internal store.

You must have CLI administrator-level access to perform import and export operations. Additionally:

- To import ACS configuration data, you need CRUD permissions for the specific configuration object.
- To export data to a remote repository, you need read permission for the specific configuration object.

This functionality is not available for all ACS objects. This section describes the supported ACS objects and how to create the import files.

This section contains:

- [Supported ACS Objects, page 5-19](#)
- [Creating Import Files, page 5-22](#)

Supported ACS Objects

While ACS 5.8.1 allows you to perform bulk operations (add, update, delete) on ACS objects using the import functionality, you cannot import all ACS objects. The import functionality in ACS 5.8.1 supports the following ACS objects:

- Users
- Hosts
- Network Devices
- Identity Groups
- NDGs
- Downloadable ACLs
- Command Sets

[Table 5-10](#) lists the ACS objects, their properties, and the property data types. The import template for each of the objects contains the properties described in this table.

**Note**

The limitations given in [Table 5-10](#) is applicable only to the internal database users and not applicable to the external database (AD, LDAP, or RSA) users.

Table 5-10 ACS Objects – Property Names and Data Types

Property Name	Property Data Type
Object Type: User	
Username	(Required in create, edit, and delete) String. Maximum length is 64 characters.
Description	(Optional) String. Maximum length is 1024 characters.
Enabled	(Required in create) Boolean.
Change Password	(Required in create) Boolean.
Password	(Required in create) String. Maximum length is 32 characters. Not available in Export.
Enable Password	(Optional) String. Maximum length is 32 characters.
Password Type	(Required in create) String. Maximum length is 256 characters.
User Identity Group	(Optional) String. Maximum length is 256 characters.
List of attributes	(Optional) String and other data types.
Object Type: Hosts	
MAC address	(Required in create, edit, delete) String. Maximum length is 64 characters.
Description	(Optional) String. Maximum length is 1024 characters.
Enabled	(Optional) Boolean.
Host Identity Group	(Optional) String. Maximum length is 256 characters.
List of attributes	(Optional) String.
Object Type: Network Device	
Name	(Required in create, edit, delete) String. Maximum length is 64 characters.
Description	(Optional) String. Maximum length is 1024 characters.
Subnet	(Required in create) Subnets IPv4: <a.b.c.d>/m excluding a.b.c.d/32; wild cards (*,-). IPv6: <a:b:c:d:e:f:g:h>/n; wild cards (:,::). The exclude range is available only for IPv4 addresses.
Support RADIUS	(Required in create) Boolean.
RADIUS secret	(Optional) String. Maximum length is 32 characters.
coaPort	(Optional) Integer.
SupportKeyWrap	(Optional) Boolean.
KeywrapKEK	(Optional) String. Maximum length is 32 characters.
KeywrapMACK	(Optional) String. Maximum length is 40 characters.
KeywrapDisplayInHex	(Optional) Boolean.
Support TACACS	(Required in create) Boolean.
TACACS secret	(Optional) String. Maximum length is 32 characters.

Table 5-10 ACS Objects – Property Names and Data Types

Property Name	Property Data Type
Single connect	(Optional) Boolean.
Legacy TACACS	(Optional) Boolean.
Support SGA	(Required in create) Boolean.
SGA Identity	(Optional) String. Maximum length is 32 characters.
SGA trusted	(Optional) Boolean.
Password	(Optional) String. Maximum length is 32 characters.
sgACLTTTL	(Optional) Integer.
peerAZNTTL	(Optional) Integer.
envDataTTL	(Optional) Integer.
Session timeout	(Optional) Integer.
List of NDG names	(Optional) String.
Location	(Optional) String. Maximum length is 32 characters.
Device Type	(Optional) String. Maximum length is 32 characters.
Object Type: Identity Group	
Name	(Required in create, edit, delete) String. Maximum length is 64 characters.
Description	(Optional) String. Maximum length is 1024 characters.
Object Type: NDG	
Name	(Required in create, edit, delete) String. Maximum length is 64 characters.
Description	(Optional) String. Maximum length is 1024 characters.
Object Type: Downloadable ACLs	
Name	(Required in create, edit, delete) String. Maximum length is 64 characters.
Description	(Optional) String. Maximum length is 1024 characters.
Content	(Required in create, edit, delete) String. The ACL content is split into permit/deny statements separated by a semicolon (;). Maximum length for each statement is 256 characters. There is no limit for ACL content.
Object Type: Command Set	
Name	(Required in create, edit, delete) String. Maximum length is 64 characters.
Description	(Optional) String. Maximum length is 1024 characters.
Commands (in the form of <i>grant:command:arguments</i>)	(Optional) String. This is a list with semi separators (;) between the values that you supply for <i>grant</i> .

Fields that are optional can be left empty and ACS substitutes the default values for those fields.

For example, when fields that are related to a hierarchy are left blank, ACS assigns the value of the root node in the hierarchy. For network devices, if Security Group Access is enabled, all the related configuration fields are set to default values.

Creating Import Files

This section describes how to create the .csv file for performing bulk operations on ACS objects. You can download the appropriate template for each of the objects from the ACS web interface. This section contains the following:

- [Downloading the Template from the Web Interface, page 5-22](#)
- [Understanding the CSV Templates, page 5-23](#)
- [Creating the Import File, page 5-23](#)

Downloading the Template from the Web Interface

Before you can create the import file, you must download the import file templates from the ACS web interface.

To download the import file templates for adding internal users:

-
- Step 1** Log into the ACS 5.8.1 web interface.
- Step 2** Choose **Users and Identity Stores > Internal Identity Stores > Users**.
The Users page appears.
- Step 3** Click **File Operations**.
The File Operations wizard appears.
- Step 4** Choose any one of the following:
- Add—Adds users to the existing list. This option does not modify the existing list. Instead, it performs an append operation.
 - Update—Updates the existing internal user list.
 - Delete—Deletes the list of users in the import file from the internal identity store.
- Step 5** Click **Next**.
The Template page appears.
- Step 6** Click **Download Add Template**.
- Step 7** Click **Save** to save the template to your local disk.
-

The following list gives you the location from which you can get the appropriate template for each of the objects:

- User—**Users and Identity Stores > Internal Identity Stores > Users**
- Hosts—**Users and Identity Stores > Internal Identity Stores > Hosts**
- Network Device—**Network Resources > Network Devices and AAA Clients**
- Identity Group—**Users and Identity Stores > Identity Groups**
- NDG
 - Location—**Network Resources > Network Device Groups > Location**
 - Device Type—**Network Resources > Network Device Groups > Device Type**

- Downloadable ACLs—**Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs**
- Command Set—**Policy Elements > Authorization and Permissions > Device Administration > Command Sets**

Follow the procedure described in this section to download the appropriate template for your object.

Understanding the CSV Templates

You can open your CSV template in Microsoft Excel or any other spreadsheet application and save the template to your local disk as a .csv file. The .csv template contains a header row that lists the properties of the corresponding ACS object.

For example, the internal user Add template contains the fields described in [Table 5-11](#):

Table 5-11 Internal User Add Template

Header Field	Description
name:String(64):Required	Username of the user.
description:String(1024)	Description of the user.
enabled:Boolean (True,False):Required	Boolean field that indicates whether the user must be enabled or disabled.
changePassword:Boolean (True,False):Required	Boolean field that indicates whether the user must change password on first login.
password:String(32):Required	Password of the user.
enablePassword:String(32)	Enable password of the user.
UserIdentityGroup:String(256)	Identity group to which the user belongs.
All the user attributes that you have specified would appear here.	

Each row of the .csv file corresponds to one internal user record. You must enter the values into the .csv file and save it before you can import the users into ACS. See [Creating the Import File, page 5-23](#) for more information on how to create the import file.

This example is based on the internal user Add template. For the other ACS object templates, the header row contains the properties described in [Table 5-10](#) for that object.

Creating the Import File

After you download the import file template to your local disk, enter the records that you want to import into ACS in the format specified in the template. After you enter all the records into the .csv file, you can proceed with the import function. The import process involves the following:

- [Adding Records to the ACS Internal Store, page 5-23](#)
- [Updating the Records in the ACS Internal Store, page 5-24](#)
- [Deleting Records from the ACS Internal Store, page 5-25](#)

Adding Records to the ACS Internal Store

When you add records to the ACS internal store, you add the records to the existing list. This is an append operation, in which the records in the .csv file are added to the list that exists in ACS.

To add internal user records to the Add template:

- Step 1** Download the internal user Add template. See [Downloading the Template from the Web Interface](#), page 5-22 for more information.
- Step 2** Open the internal user Add template in Microsoft Excel or any other spreadsheet application. See [Table 5-10](#) for a description of the fields in the header row of the template.
- Step 3** Enter the internal user information. Each row of the .csv template corresponds to one user record. [Figure 5-12](#) shows a sample Add Users import file.

Figure 5-12 Add Users – Import File

	A	B	C	D	E	F	G	H	I	J	K
1	name:String(64);Re:description:String(256);enabled:changePasswpassword:String(256);enablePasswoUseridentityGroup:String(256);attr-Real Nameattr-Description:String(256)										
2	John		TRUE	FALSE	1234		All Groups:SanJose				
3	Kenneth		TRUE	FALSE	1235		All Groups:SanJose				
4	Abraham		TRUE	FALSE	1236		All Groups:Texas				
5	Kelly		TRUE	FALSE	1237		All Groups:Texas				
6	Sandra		TRUE	FALSE	1238		All Groups:Florida				
7	Nilofer		TRUE	FALSE	1239		All Groups:Florida				
8	James		TRUE	FALSE	1240		All Groups:SanJose				
9	Albert		TRUE	FALSE	1241		All Groups:Florida				
10	Kevin		TRUE	FALSE	1242		All Groups:Florida				
11	Samantha		TRUE	FALSE	1243		All Groups:Texas				

- Step 4** Save the add users import file to your local disk.

Updating the Records in the ACS Internal Store

When you update the records in the ACS store, the import process overwrites the existing records in the internal store with the records from the .csv file. This operation replaces the records that exist in ACS with the records from the .csv files.

The update operation is similar to the add operation except for one additional column that you can add to the Update templates. The Update template can contain an Updated name column for internal users and other ACS objects, and an Updated MAC address column for the internal hosts. The Updated Name replaces the name.



Note

Instead of downloading the update template for each of the ACS objects, you can use the export file of that object, retain the header row, and update the data to create your update .csv file.

To add an updated name or MAC address to the ACS objects, you have to download and use the particular update template. Also, for the NDGs, the export template contains only the NDG name, so in order to update any other property, you must download and use the NDG update template.

For example, [Figure 5-13](#) shows a sample import file that updates existing user records.

Figure 5-13 *Update Users–Import File*

	A	B	C	D	E	F	G	H	I	J	K	L
1	name:String	Updated name:String	description enabled:Boolean	changePassword:enablePassword	UserIdentifier-Real Name	Description:String(256)						
2	John	Mark		TRUE	FALSE	1234		All Groups:SanJose				
3	Kenneth	David		TRUE	FALSE	1235		All Groups:SanJose				
4	Abraham	Jamie		TRUE	FALSE	1236		All Groups:Texas				
5	Kelly	Lucy		TRUE	FALSE	1237		All Groups:Texas				
6	Sandra	Tina		TRUE	FALSE	1238		All Groups:Florida				
7	Nilofer	William		TRUE	FALSE	1239		All Groups:Florida				
8	James	Frank		TRUE	FALSE	1240		All Groups:SanJose				
9	Albert	George		TRUE	FALSE	1241		All Groups:Florida				
10	Kevin	Paul		TRUE	FALSE	1242		All Groups:Florida				
11	Samantha	Patrick		TRUE	FALSE	abcd		All Groups:Texas				

**Note**

The second column, Updated name, is the additional column that you can add to the Update template.

Deleting Records from the ACS Internal Store

You can use this option to delete a subset of records from the ACS internal store. The records that are present in the .csv file that you import are deleted from the ACS internal store. The Delete template contains only the key column to identify the records that must be deleted.

For example, to delete a set of internal users from the ACS internal identity store, download the internal user Delete template and add the list of users that you want to delete to this import file. [Figure 5-14](#) shows a sample import file that deletes internal user records.

**Note**

To delete all users, you can export all users and then use the same export file as your import file to delete users.

Figure 5-14 *Delete Users – Import File*

	A	B	C	D	E	F
1	name:String(64):Required					
2	kenneth					
3	jamie					
4	john					
5	joseph					
6	nilofer					
7	casey					
8	lucie					
9	jacob					
10	george					

Common Errors

You might encounter these common errors:

- [Concurrency Conflict Errors, page 5-26](#)
- [Deletion Errors, page 5-27](#)
- [System Failure Errors, page 5-27](#)
- [Accessibility, page 5-28](#)

Concurrency Conflict Errors

Concurrency conflict errors occur when more than one user tries to update the same object. When you click **Submit** and the web interface detects an error, a dialog box appears, with an error message and an **OK** button. Read the error message, click **OK**, and resubmit your configuration, if needed.

Possible error messages, explanations, and recommended actions are:

Error Message The item you are trying to Submit has been modified elsewhere while you were making your changes.

Explanation You accessed an item to perform an edit and began to configure it; simultaneously, another user accessed and successfully submitted a modification to it. Your submission attempt failed.

Recommended Action Click **OK** to close the error message and display the content area list page. The page contains the latest version of all items. Resubmit your configuration, if needed.

Error Message The item you are trying to Submit has been deleted while you were making your changes.

Explanation If you attempt to submit an edited item that another user simultaneously accessed and deleted, your submission attempt fails. This error message appears in a dialog box with an **OK** button.

Recommended Action Click **OK** to close the error message and display the content area list page. The page contains the latest version of all items. The item that you tried to submit is not saved or visible.

Error Message The item you are trying to Duplicate from has been deleted.

Error Message The item you are trying to Edit has been deleted.

Explanation You attempted to duplicate or edit a selected item that another user deleted at the same time that you attempted to access it.

Recommended Action Click **OK** to close the error message and display the content area list page. The page contains the latest version of all items. The item that you tried to duplicate or edit is not saved or visible.

Error Message The item you are trying to Submit is referencing items that do not exist anymore.

Explanation You attempted to edit or duplicate an item that is referencing an item that another user deleted while you tried to submit your change.

Recommended Action Click **OK** to close the error message and display the previous page, the Create page or the Edit page. Your attempted changes are not saved, nor do they appear in the page.

Error Message Either Import or Export is already in progress.

Explanation You attempted to import or export a .csv file while a previous import or export is still in progress. The subsequent import or export will not succeed. The original import or export is not interrupted due to this error.

Recommended Action Click **OK** to close the error message and display the previous page. For a currently running import process, consult the Import Progress secondary window and wait for the Save Log button to become enabled. Save the log, then attempt to import or export your next .csv file.

Deletion Errors

Deletion errors occur when you attempt to delete an item (or items) that another item references. When you click **Delete** and an error is detected, a dialog box appears, with an error message and an **OK** button. Read the error message, click **OK**, and perform the recommended action.

Possible error messages, explanations, and recommended actions are:

Error Message The item you are trying to Delete is referenced by other Items. You must remove all references to this item before it can be deleted.

Error Message Some of the items you are trying to Delete are referenced by other Items. You must remove all references to the items before they can be deleted.

Explanation If you attempt to delete one or more items that another item references, the system prevents the deletion.

Recommended Action Click **OK** to close the error message and display the content area list page. Your deletion does not occur and the items remain visible in the page. Remove all references to the item or items you want to delete, then perform your deletion.

System Failure Errors

System failure errors occur when a system malfunction is detected. When a system failure error is detected, a dialog box appears, with an error message and OK button. Read the error message, click **OK**, and perform the recommended action.

Possible error messages, explanations, and recommended actions are:

Error Message The following System Failure occurred: *<description>*.

Where *description* describes the specific malfunction.

Explanation You have attempted to make a configuration change and the system detected a failure at the same time.

Recommended Action Click **OK** to close the error message and display the content area list page. Your changes are not saved. Investigate and troubleshoot the detected malfunction, if possible.

Error Message An unknown System Failure occurred.

Explanation You tried to change the configuration and the system detected an unknown failure at the same time.

Recommended Action Click **OK** to close the error message and display the content area list page. Investigate possible system failure causes, if possible.

Accessibility

The ACS 5.8.1 web interface contains accessibility features for users with vision impairment and mobility limitations.

This section contains the following topics:

- [Display and Readability Features, page 5-28](#)
- [Keyboard and Mouse Features, page 5-28](#)
- [Obtaining Additional Accessibility Information, page 5-29](#)

Display and Readability Features

The ACS 5.8.1 web interface includes features that:

- Increase the visibility of items on the computer screen.
- Allow you to use screen reader software to interpret the web interface text and elements audibly.

The display and readability features include:

- Useful text descriptions that convey information that appears as image maps and graphs.
- Meaningful and consistent labels for tables, buttons, fields, and other web interface elements.
- Label placement directly on, or physically near, the element to which they apply.
- Color used as an enhancement of information only, not as the only indicator. For example, required fields are associated with a red asterisk.
- Confirmation messages for important settings and actions.
- User-controllable font, size, color, and contrast of the entire web interface.

Keyboard and Mouse Features

You can interact with the ACS 5.8.1 web interface by using the keyboard and the mouse to accomplish actions. The keyboard and mouse features include:

- Keyboard accessible links to pages that display dynamic content.
- Standard keyboard equivalents are available for all mouse actions.
- Multiple simultaneous keystrokes are not required for any action.
- Pressing a key for an extended period of time is not required for any action.
- Backspace and deletion are available for correcting erroneous entries.

Obtaining Additional Accessibility Information

For more information, refer to the Cisco Accessibility Program:

- E-mail: accessibility@cisco.com
- Web: <http://www.cisco.com/go/accessibility>



Post-Installation Configuration Tasks

This chapter provides a set of configuration tasks that you must perform to work with ACS. This chapter contains the following sections:

- [Configuring Minimal System Setup, page 6-1](#)
- [Configuring ACS to Perform System Administration Tasks, page 6-1](#)
- [Configuring ACS to Manage Access Policies, page 6-3](#)
- [Configuring ACS to Monitor and Troubleshoot Problems in the Network, page 6-4](#)

Configuring Minimal System Setup

[Table 6-1](#) lists the steps that you must follow for a minimal system setup to get ACS up and running quickly in a lab, evaluation, or demonstration environment.

Table 6-1 *Minimal System Setup*

Step No.	Task	Drawer	Refer to...
Step 1	Add network devices.	Network Resources > Network Devices and AAA Clients	Creating, Duplicating, and Editing Network Devices, page 7-10.
Step 2	Add users.	Users and Identity Stores > Internal Identity Stores > Users	Creating Internal Users, page 8-13.
Step 3	Create authorization rules to permit or deny access.	Policy Elements > Authorization and Permissions	Managing Authorizations and Permissions, page 9-17.

Configuring ACS to Perform System Administration Tasks

[Table 6-2](#) lists the set of system administration tasks that you must perform to administer ACS.

Table 6-2 System Administration Tasks

Step No.	Task	Drawer	Refer to...
Step 1	Install ACS license.	System Administration > Configuration > Licensing	Licensing Overview, page 18-37.
Step 2	Install system certificates.	System Administration > Configuration > Local Server Certificates > Local Certificates	Configuring Local Server Certificates, page 18-16.
Step 3	Configure password policy rules for administrators and users.	<ul style="list-style-type: none"> For administrators: System Administration > Administrators > Settings > Authentication For administrator access settings: System Administration > Administrators > Settings > Access For users: System Administration > Users > Authentication Settings For hosts: System Administration > Hosts > Authentication Settings 	<ul style="list-style-type: none"> For administrators: Configuring Authentication Settings for Administrators, page 16-14. For administrator access settings: Configuring Administrator Access Settings, page 16-17 For users: Configuring Authentication Settings for Users, page 8-9.
Step 4	Add ACS administrators.	System Administration > Administrators > Accounts	Configuring System Administrators and Accounts, page 16-3
Step 5	Configure primary and secondary ACS instances.	System Administration > Operations > Distributed System Management	Understanding Distributed Deployment, page 17-2.
Step 6	Configure logging.	System Administration > Configuration > Log Configuration	Configuring Local and Remote Log Storage, page 18-23.
Step 7	Add network devices.	Network Resources > Network Devices and AAA Clients	Creating, Duplicating, and Editing Network Devices, page 7-10.

Table 6-2 System Administration Tasks (continued)

Step No.	Task	Drawer	Refer to...
Step 8	Add users or hosts to the internal identity store, or define external identity stores, or both.	<ul style="list-style-type: none"> For internal identity stores: Users and Identity Stores > Internal Identity Stores For external identity stores: Users and Identity Stores > External Identity Stores 	<ul style="list-style-type: none"> For internal identity stores: <ul style="list-style-type: none"> Creating Internal Users, page 8-13. Creating Hosts in Identity Stores, page 8-23. For external identity stores: <ul style="list-style-type: none"> Creating External LDAP Identity Stores, page 8-34. Joining ACS to an AD Domain, page 8-67. Creating and Editing RSA SecurID Token Servers, page 8-81. Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-90.
Step 9	Add end user certificates.	Users and Identity Stores > Certificate Authorities	Adding a Certificate Authority, page 8-95.
Step 10	Configure identity sequence.	Users and Identity Stores > Identity Store Sequences	Creating, Duplicating, and Editing Identity Store Sequences, page 8-102.

Configuring ACS to Manage Access Policies

[Table 6-3](#) lists the set of tasks that you must perform to manage access restrictions and permissions.

Table 6-3 Managing Access Policies

Step No.	Task	Drawer	Refer to...
Step 1	Define policy conditions.	Policy Elements > Session Conditions	Managing Policy Conditions, page 9-1.

Table 6-3 Managing Access Policies (continued)

Step No.	Task	Drawer	Refer to...
Step 2	Define authorization and permissions.	Policy Elements > Authorization and Permissions	Managing Authorizations and Permissions, page 9-17.
Step 3	Define access services and service selection policies.	Access Policies > Access Services	<ul style="list-style-type: none"> To configure access services: Configuring Access Services, page 10-11. To configure access service policies: Configuring Access Service Policies, page 10-23. To configure compound conditions: Configuring Compound Conditions, page 10-41.

Configuring ACS to Monitor and Troubleshoot Problems in the Network

[Table 6-4](#) lists a set of configuration tasks that you must perform to troubleshoot the Monitoring and Report Viewer.

Table 6-4 Monitoring and Troubleshooting Configuration

Step No.	Task	Drawer	Refer to...
Step 1	Configure data purge and backup.	Monitoring Configuration > System Operations > Data Management > Removal and Backup	Configuring Data Purging and Incremental Backup, page 15-3.
Step 2	Specify e-mail settings.	Monitoring Configuration > System Configuration > Email Settings	Specifying E Mail Settings, page 15-16.
Step 3	Configure collection filters.	Monitoring Configuration > System Configuration > Collection Filters	Understanding Collection Filters, page 15-19.
Step 4	Enable system alarms and specify how you would like to receive notification.	Monitoring Configuration > System Configuration > System Alarm Settings	Configuring System Alarm Settings, page 15-21.

Table 6-4 Monitoring and Troubleshooting Configuration (continued)

Step No.	Task	Drawer	Refer to...
Step 5	Define schedules and create threshold alarms.	Monitoring and Reports > Alarms	<ul style="list-style-type: none"> To configure schedules: Understanding Alarm Schedules, page 12-8. To create threshold alarms: Creating, Editing, and Duplicating Alarm Thresholds, page 12-11.
Step 6	Configure alarm syslog targets.	Monitoring Configuration > System Configuration > Alarm Syslog Targets	Configuring Alarm Syslog Targets, page 15-21.
Step 7	Configure remote database to export the Monitoring and Report Viewer data.	Monitoring Configuration > System Configuration > Remote Database Settings	Configuring Remote Database Settings, page 15-21.



Managing Network Resources

The Network Resources drawer defines elements within the network that issue requests to ACS or those that ACS interacts with as part of processing a request. This includes the network devices that issue the requests and external servers, such as a RADIUS server that is used as a RADIUS proxy.

This drawer allows you to configure:

- Network device groups—Logically groups the network devices, which you can then use in policy conditions.
- Network devices—Definition of all the network devices in the ACS device repository that accesses the ACS network.
- Default network device—A default network device definition that ACS can use for RADIUS or TACACS+ requests when it does not find the device definition for a particular IP address.
- External proxy servers—RADIUS servers that can be used as a RADIUS proxy.
- OCSP services—Online Certificate Status Protocol (OCSP) services are used to check the status of x.509 digital certificates and can be used as an alternate to the certificate revocation list (CRL).

When ACS receives a request from a network device to access the network, it searches the network device repository to find an entry with a matching IP address. ACS then compares the shared secret with the secret retrieved from the network device definition.

If they match, the network device groups that are associated with the network device are retrieved and can be used in policy decisions. See [ACS 5.x Policy Model, page 3-1](#) for more information on policy decisions.

The Network Resources drawer contains:

- [Network Device Groups, page 7-1](#)
- [Network Devices and AAA Clients, page 7-5](#)
- [Configuring a Default Network Device, page 7-18](#)
- [Working with External Proxy Servers, page 7-19](#)
- [Working with OCSP Services, page 7-22](#)

Network Device Groups

In ACS, you can define network device groups (NDGs), which are sets of devices. These NDGs provide logical grouping of devices, for example, Device Location or Type, which you can use in policy conditions.

When the ACS receives a request for a device, the network device groups associated with that device are retrieved and compared against those in the policy table. With this method, you can group multiple devices and assign them the same policies. For example, you can group all devices in a specific location together and assign to them the same policy.

The Device Group Hierarchy is the hierarchical structure that contains the network device groups. Two of these, *Location* and *Device Type*, are predefined; you can edit their names but you cannot delete them. You can add up to 6 additional hierarchies including the root.

An NDG relates to any node in the hierarchy and is the entity to which devices are associated. These nodes can be any node within the hierarchy, not just leaf nodes.

**Note**

You can have a maximum of six nodes in the NDG hierarchy, including the root node.

Related Topics

- [Creating, Duplicating, and Editing Network Device Groups, page 7-2](#)
- [Deleting Network Device Groups, page 7-3](#)

Creating, Duplicating, and Editing Network Device Groups

To create, duplicate, or edit a network device group:

Step 1 Choose **Network Resources > Network Device Groups**.

The Network Device Groups page appears. If you have defined additional network device groups, they appear in the left navigation pane, beneath the Network Device Groups option.

Step 2 Do any of the following:

- Click **Create**.
- Check the check box the network device group that you want to duplicate, then click **Duplicate**.
- Click the network device group name that you want to modify, or check the check box the name and click **Edit**.

The Hierarchy - General page appears.

Step 3 Modify the fields in the Hierarchy - General page as described in [Table 7-1 on page 2](#):

Table 7-1 *Device Groups - General Page Field Descriptions*

Field	Description
Name	Enter a name for the network device group (NDG).
Description	(Optional) Enter a description for the NDG.
Root Node Name/Parent	Enter the name of the root node associated with the NDG. The NDG is structured as an inverted tree, and the root node is at the top of the tree. The root node name can be the same as the NDG name. The NDG name is displayed when you click an NDG in the Network Resources drawer.

Step 4 Click **Submit**.

The network device group configuration is saved. The Network Device Groups page appears with the new network device group configuration.

Related Topics

- [Network Device Groups, page 7-1](#)
- [Deleting Network Device Groups, page 7-3](#)
- [Creating, Duplicating, and Editing Network Device Groups Within a Hierarchy, page 7-3](#)
- [Performing Bulk Operations for Network Resources and Users, page 7-8](#)

Deleting Network Device Groups

To delete a network device group:

Step 1 Choose **Network Resources > Network Device Groups**.

The Network Device Groups page appears.

Step 2 Check one or more check boxes the network device groups you want to delete, and click **Delete**.

The following error message appears:

Error Message You have requested to delete a network device group. If this group is referenced from a Policy or a Policy Element then the delete will be prohibited. If this group is referenced from a network device definition, the network device will be modified to reference the root node name group.

Step 3 Click **OK**.

The Network Device Groups page appears without the deleted network device groups.

Creating, Duplicating, and Editing Network Device Groups Within a Hierarchy

You can arrange the network device group node hierarchy according to your needs by choosing parent and child relationships for new, duplicated, or edited network device group nodes. You can also delete network device group nodes from a hierarchy.

To create, duplicate, or edit a network device group node within a hierarchy:

Step 1 Choose **Network Resources > Network Device Groups**.

The Network Device Groups page appears.

Step 2 Click **Location**, **Device Type**, or another previously defined network device group in which you want to create a new network device group, and add it to the hierarchy of that group.

The Network Device Group hierarchy page appears.

Step 3 Do one of the following:

- Click **Create**. If you click **Create** when you have a group selected, the new group becomes a child of the parent group you selected. You can move a parent and all its children around in the hierarchy by clicking **Select** from the Create screen.
- Check the check box the network device group name that you want to duplicate, then click **Duplicate**.
- Click the network device group name that you want to modify, or check the check box the name and click **Edit**.

The Device Group - General page appears.

Step 4 Modify fields in the Device Groups - General page as shown in [Table 7-2](#):

Table 7-2 *Device Groups - General Page Field Descriptions*

Field	Description
Name	Enter a name for the NDG.
Description	(Optional) Enter a description for the NDG.
Parent	Enter the name of the parent associated with the NDG. The NDG is structured as an inverted tree, and the parent name is the name of the top of the tree. Click Select to open the Groups dialog box from which you can select the appropriate parent for the group.

Step 5 Click **Submit**.

The new configuration for the network device group is saved. The Network Device Groups hierarchy page appears with the new network device group configuration.

Related Topics

- [Network Device Groups, page 7-1](#)
- [Deleting Network Device Groups, page 7-3](#)
- [Creating, Duplicating, and Editing Network Device Groups, page 7-2](#)
- [Performing Bulk Operations for Network Resources and Users, page 7-8](#)

Deleting Network Device Groups from a Hierarchy

To delete a network device group from within a hierarchy:

Step 1 Choose **Network Resources > Network Device Groups**.

The Network Device Groups page appears.

Step 2 Click **Location**, **Device Type**, or another previously defined network device group in which you want to edit a network device group node.

The Network Device Groups node hierarchy page appears.

Step 3 Select the nodes that you want to delete and click **Delete**.

The following message appears:

You have requested to delete a network device group. If this group is referenced from a Policy or a Policy Element then the delete will be prohibited. If this group is referenced from a network device definition, the network device will be modified to reference the root node name group.

Step 4 Click **OK**.



Note Root node of a group cannot be deleted from NDG hierarchy. If you try to do so, the following error message appears:
Selected node can be removed only with a root group.

The network device group node is removed from the configuration. The Network Device Groups hierarchy page appears without the device group node that you deleted.

Network Devices and AAA Clients

You must define all devices in the ACS device repository that access the network. The network device definition can be associated with a specific IP address or a subnet mask, where all IP addresses within the subnet can access the network.

The device definition includes the association of the device to network device groups (NDGs). You also configure whether the device uses TACACS+ or RADIUS, and if it is a Security Group Access device.



Note When you use subnet masks, the number of unique IP addresses depends on the number of IP addresses available through the subnet mask. For example, a subnet mask of 255.255.255.0 means you have 256 unique IP addresses.

You can import devices with their configurations into the network devices repository.

When ACS receives a request, it searches the network device repository for a device with a matching IP address; then ACS compares the secret or password information against that which was retrieved from the network device definition. If the information matches, the NDGs associated with the device are retrieved and can be used in policy decisions.

You must install Security Group Access license to enable Security Group Access options. The Security Group Access options only appear if you have installed the Security Group Access license. For more information on Security Group Access licenses, see [Licensing Overview, page 18-37](#).

Viewing and Performing Bulk Operations for Network Devices

You can view the network devices and AAA clients. These are the devices sending access requests to ACS. The access requests are sent via TACACS+ or RADIUS.

To view and import network devices:

Step 1 Choose **Network Resources > Network Devices and AAA Clients**.

The Network Device page appears, with any configured network devices listed. [Table 7-3](#) provides a description of the fields in the Network Device page:

Table 7-3 Network Device Page Field Descriptions

Option	Description
Name	User-specified name of network devices in ACS. Click a name to edit the associated network device (see Displaying Network Device Properties, page 7-14).
IP Address	<p><i>Display only.</i> The IP address or subnet mask of each network device. The first three IP addresses of type IPv4 or IPv6 appear in the field, each separated by a comma (,).</p> <p>If this field contains a subnet mask, all IP addresses within the specified subnet mask are permitted to access the network and are associated with the network device definition.</p> <p>When you use subnet masks, the number of unique IP addresses depends on the number of IP addresses that are available through the subnet mask. For example:</p> <p>IPv4—A subnet mask of 255.255.255.0 means you have 256 unique IPv4 addresses. By default, the subnet mask value for IPv4 is 32.</p> <p>IPv6—A subnet mask of 2001:0DB8:0:CD30::/127 means you have 2 unique IPv6 addresses. By default, the subnet mask value for IPv6 is 128.</p> <p>You can see the excluded IP address the specified IP address, if any.</p>
NDG: <i>string</i>	Network device group. The two predefined NDGs are Location and Device Type. If you have defined additional network device groups, they are listed here as well.
Description	<i>Display only.</i> Descriptions of the network devices.

Step 2 Do any one of the following:

- Click **Create** to create a new network device. See [Creating, Duplicating, and Editing Network Devices, page 7-10](#).
- Check the check box the network device that you want to edit and click **Edit**. See [Creating, Duplicating, and Editing Network Devices, page 7-10](#).
- Check the check box the network device that you want to duplicate and click **Duplicate**. See [Creating, Duplicating, and Editing Network Devices, page 7-10](#).
- Search for the Network devices based on the following categories:
 - Name
 - IP Address
 - Description
 - NDG Location
 - Device Type

You can specify full IP address, or IP address with wildcard “*” or, with IP address range, such as [15-20] in the IP address search field. The wildcard “*” and the IP range [15-20] option can be specified in all the 4 octets of IP address. The Equals option only is listed in the search condition when searching by IP address.

**Note**

When you search for an IP address or IP-Range address, the search result displays all records that match the Search criteria, even if the Search IP Address (or) IP-Range address is in Excluded IP Address (or) Range.

- Click **File Operations** to perform any of the following functions:

- Add—Choose this option to add a list of network devices from the import file in a single shot.
- Update—Choose this option to replace the list of network devices in ACS with the network devices in the import file.
- Delete—Choose this option to delete from ACS the network devices listed in the import file.

See [Performing Bulk Operations for Network Resources and Users](#), page 7-8 for more information.

For information on how to create the import files, refer to [Software Developer's Guide for Cisco Secure Access Control System](#).

**Note**

To perform a bulk add, edit, or delete operation on any of the ACS objects, you can use the export file of that object, retain the header row, and create the .csv import file. However, to add an updated name or MAC address to the ACS objects, must to download and use the particular update template. Also, for the NDGs, the export template contains only the NDG name, so in order to update any other property, you must download and use the NDG update template.

Related Topics:

- [Network Devices and AAA Clients](#), page 7-5
- [Performing Bulk Operations for Network Resources and Users](#), page 7-8
- [Creating, Duplicating, and Editing Network Device Groups Within a Hierarchy](#), page 7-3

Exporting Network Devices and AAA Clients

**Note**

You must turn off the popup blockers in your browser to ensure that the export process completes successfully.

To export a list of network devices:

- Step 1** Choose **Network Resources > Network Devices and AAA Clients**.
The Network Device page appears.
- Step 2** Choose the filter condition and the Match if operator, and enter the filter criterion that you are looking for in the text box.
- Step 3** Click **Go**.
A list of records that match your filter criterion appears. You can export this list to a .csv file.
- Step 4** Click **Export** to export the records to a .csv file.
A system message box appears, prompting you for an encryption password to encrypt the .csv file during file transfer.
- Step 5** To encrypt the export .csv file, check the **Password** check box and enter the encryption password. You can optionally choose to not encrypt the file during transfer.
- Step 6** Click **Start Export** to begin the export process.
The Export Progress window appears, displaying the progress of the export process. If any errors are encountered during this process, they are displayed in the Export Progress window.

You can terminate the export process at any time during this process. All the reports, till you abort the export process, get exported. To resume, you have to start the export process all over again.

- Step 7** After the export process is complete, Click **Save File** to save the export file to your local disk. The export file is a .csv file that is compressed as export.zip.
-

Performing Bulk Operations for Network Resources and Users

You can use the file operation function to perform bulk operations (add, update, and delete) for the following on your database:

- Internal users
- Internal hosts
- Network devices

For bulk operations, you must download the .csv file template from ACS and add the records that you want to add, update, or delete to the .csv file and save it to your local disk. Use the Download Template function to ensure that your .csv file adheres to the requirements.

The .csv templates for users, internal hosts, and network devices are specific to their type; for example, you cannot use a downloaded template accessed from the Users page to add internal hosts or network devices. Within the .csv file, you must adhere to these requirements:

- Do not alter the contents of the first record (the first line, or row, of the .csv file).
- Use only one line for each record.
- Do not imbed new-line characters in any fields.
- For non-English languages, encode the .csv file in utf-8 encoding, or save it with a font that supports Unicode.

Before you begin the bulk operation, ensure that your browser's popup blocker is disabled.

- Step 1** Click **File Operations** on the Users, Network Devices, or MAC Address page of the web interface. The Operation dialog box appears.
- Step 2** Click **Next** to download the .csv file template if you do not have it.
- Step 3** Click any one of the following operations if you have previously created a template-based .csv file on your local disk:
- Add—Adds the records in the .csv file to the records currently available in ACS.
 - Update—Overwrites the records in ACS with the records from the .csv file.
 - Delete—Removes the records in the .csv file from the list in ACS.
- Step 4** Click **Next** to move to the next page.
- Step 5** Click **Browse** to navigate to your .csv file.
- Step 6** Choose either of the following options that you want ACS to follow in case of an error during the import process:
- Continue processing remaining records; successful records will be imported.
 - Stop processing the remaining records; only the records that were successfully imported before the error will be imported.

- Step 7** Check the **Password** check box and enter the password to decrypt the .csv file if it is encrypted in GPG format.
- Step 8** Click **Finish** to start the bulk operation.
- The Import Progress window appears. Use this window to monitor the progress of the bulk operation. Data transfer failures of any records within your .csv file are displayed.
- You can click the Abort button to stop importing data that is under way; however, the data that was successfully transferred is not removed from your database.
- When the operation completes, the Save Log button is enabled.
- Step 9** Click **Save Log** to save the log file to your local disk.
- Step 10** Click **OK** to close the Import Progress window.
- You can submit only one .csv file to the system at one time. If an operation is under way, an additional operation cannot succeed until the original operation is complete.

**Note**

Internal users whose password type is NAC Profiler can also be imported when NAC Profiler is not installed in ACS.

For information on how to create the import files, refer to [Software Developer's Guide for Cisco Secure Access Control System](#).

**Note**

To perform a bulk add, edit, or delete operation on any of the ACS objects, you can use the export file of that object, retain the header row, and create the .csv import file. However, to add an updated name or MAC address to the ACS objects, you must download and use the particular update template. Also, for the NDGs, the export template contains only the NDG name, so in order to update any other property, you must download and use the NDG update template.

Exporting Network Resources and Users

To export a list of network resources or users:

- Step 1** Click **Export** on the Users, Network Devices, or MAC Address page of the web interface.
- The Network Device page appears.
- Step 2** Choose the filter condition and the Match if operator, and enter the filter criterion that you are looking for in the text box.
- Step 3** Click **Go**.
- A list of records that match your filter criterion appears. You can export these to a .csv file.
- Step 4** Click **Export** to export the records to a .csv file.
- A system message box appears, prompting you for an encryption password to encrypt the .csv file during file transfer.
- Step 5** To encrypt the export .csv file, check the **Password** check box and enter the encryption password. You can optionally choose to not encrypt the file during transfer.
- Step 6** Click **Start Export** to begin the export process.

The Export Progress window appears, displaying the progress of the export process. If any errors are encountered during this process, they are displayed in the Export Progress window.

You can terminate the export process at any time during this process. If you terminate the export process, all the reports till the termination of the process are exported. If you want to resume, you have to start the export process all over again.

- Step 7** After the export process is complete, Click **Save File** to save the export file to your local disk.
The export file is a .csv file that is compressed as export.zip.
-

Creating, Duplicating, and Editing Network Devices

You can use the bulk import feature to import a large number of network devices in a single operation; see [Performing Bulk Operations for Network Resources and Users, page 7-8](#) for more information. Alternatively, you can use the procedure described in this topic to create network devices.

To create, duplicate, or edit a network device:

-
- Step 1** Choose **Network Resources > Network Devices and AAA Clients**.
- The Network Devices page appears, with a list of your configured network devices, if any.
- Step 2** Do one of the following:
- Click **Create**.
 - Check the check box the network device name that you want to duplicate, then click **Duplicate**.
 - Click the network device name that you want to modify, or check the check box the name and click **Edit**.
- The first page of the Create Network Device process appears if you are creating a new network device. The Network Device Properties page for the selected device appears if you are duplicating or editing a network device.
- Step 3** Modify the fields as required. For field descriptions, see [Configuring Network Device and AAA Clients, page 7-10](#).
- Step 4** Click **Submit**.
- Your new network device configuration is saved. The Network Devices page appears, with your new network device configuration listed.
-

Related Topics

- [Viewing and Performing Bulk Operations for Network Devices, page 7-5](#)
- [Configuring Network Device and AAA Clients, page 7-10](#)

Configuring Network Device and AAA Clients

To display this page, choose **Network Resources > Network Devices and AAA Clients**, then click **Create**.

Table 7-4 Creating Network Devices and AAA Clients


Option	Description
General	
Name	Name of the network device. If you are duplicating a network device, you must enter a unique name as a minimum configuration; all other fields are optional.
Description	Description of the network device.
Network Device Groups¹	
Location	Click Select to display the Network Device Groups selection box. Click the radio button the Location network device group you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
Device Type	Click Select to display the Network Device Groups selection box. Click the radio button the Device Type network device group you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
IP Address	
The IP addresses and subnet masks that are associated with the network device. Select to enter a single IP address or to define a range.	
Single IP Address	<p>Choose to enter a single IP address. The IP address can be either IPv4 or IPv6. ACS 5.8.1 validates the IP address if the address is entered in the supported format. It displays an error message if the entered format is not correct.</p> <p>In ACS 5.8.1, you can configure a network device with a single static IP address that can be part of a IP subnet or range configured on another network device. For more information, see Using Single Static IP Addresses That Are Part of IP Subnets and IP Ranges, page 7-17.</p> <div>  <p>Note IPv6 addresses are supported only in TACACS+ protocols.</p> </div>
IP Subnets	<p>Choose to enter an IP address range. You can configure up to 40 IP addresses or subnet masks for each network device. If you use a subnet mask in this field, all IP addresses within the specified subnet mask are permitted to access the network and are associated with the network device definition.</p> <p>When you use subnet masks, the number of unique IP addresses depends on the number of IP addresses available through the subnet mask. For example, a subnet mask of 255.255.255.0 means you have 256 unique IP addresses. By default, the subnet mask value for IPv4 is 32, and the IPv6 value is 128.</p> <p>The first six IP addresses appear in the field; use the scroll bar to see any additional configured IP addresses.</p> <p>A mask is needed only for wildcards, if you want an IP address range. You cannot use an asterisk (*) as a wildcard.</p>

Table 7-4 Creating Network Devices and AAA Clients (continued)


Option	Description
IP Range(s)	<p>Choose to enter single or multiple ranges of IP address. You can configure up to 40 IP addresses or subnet masks for each network device. You can also exclude a subnet of IP address range from the configured range in a scenario where that subset has already been added.</p> <p>You can use a hyphen (-) to specify a range of IP addresses. A maximum of 40 IP addresses are allowed in a single IP range.</p> <p>You can also add IP addresses with wildcards. You can use asterisks (*) as wildcards.</p> <p>Some examples of entering IP address ranges are:</p> <ul style="list-style-type: none"> • A single range—10.77.10.1-10,,, 192.120.10-12.10 • Multiple ranges—10.*.1-20.10, 192.1-23.*.100-150 • Exclusions from a range—10.10.1-255.* exclude 10.10.10-200.100-150 <p>Using dynamic device IP address ranges (for example: 1-5.*.7.9) can have performance implications on both the run-time and the management.</p> <p>Therefore, we recommend using IP address and subnet mask whenever possible. The dynamic IP address ranges should be used only when the range cannot be described using IP address and subnet mask.</p> <div>  <p>Note AAA clients with wildcards are migrated from 4.x to 5.x.</p> </div>
Authentication Options	
TACACS+	<p>Check to use the Cisco IOS TACACS+ protocol to authenticate communication to and from the network device.</p> <p>You must use this option if the network device is a Cisco device-management application, such as Management Center for Firewalls. You should use this option when the network device is a Cisco access server, router, or firewall.</p> <p>Check TACACS+ if you use IPv4 or IPv6 IP addresses.</p>
TACACS+ Shared Secret	<p>Shared secret of the network device, if you enabled the TACACS+ protocol.</p> <p>A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.</p>
Single Connect Device	<p>Check to use a single TCP connection for all TACACS+ communication with the network device. Choose one:</p> <ul style="list-style-type: none"> • Legacy TACACS+ Single Connect Support • TACACS+ Draft Compliant Single Connect Support <p>If you disable this option, a new TCP connection is used for every TACACS+ request.</p>
RADIUS	<p>Check to use the RADIUS protocol to authenticate communication to and from the network device.</p> <p>Uncheck this option if you use an IPv6 address.</p>
RADIUS Shared Secret	<p>Shared secret of the network device, if you have enabled the RADIUS protocol.</p> <p>A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.</p>

Table 7-4 Creating Network Devices and AAA Clients (continued)

Option	Description
CoA Port	Used to set up the RADIUS CoA port for session directory, for user authentication. This session directory can be launched from Monitoring and Troubleshooting Viewer page. By default, the CoA port value is filled as 1700.
Enable KeyWrap	Check to enable the shared secret keys for RADIUS KeyWrap in PEAP, EAP-FAST and EAP-TLS authentications. Each key must be unique, and must also be distinct from the RADIUS shared key. These shared keys are configurable for each AAA Client. The default key mode for KeyWrap is hexadecimal string.
Key Encryption Key (KEK)	Used for encryption of the Pairwise Master Key (PMK). In ASCII mode, enter a key length of exactly 16 characters; in hexadecimal mode, enter a key length of 32 characters.
Message Authentication Code Key (MACK)	Used to calculate the keyed hashed message authentication code (HMAC) over the RADIUS message. In ASCII mode, enter a key length with 20 characters. In hexadecimal mode, enter a key with 40 characters.
Key Input Format	Enter the keys as ASCII or hexadecimal strings. The default is hexadecimal.
Security Group Access	Appears only when you enable the Cisco Security Group Access feature. Check to use Security Group Access functionality on the network device. If the network device is the seed device (first device in the Security Group Access network), you must also check the RADIUS check box.
Use Device ID for Security Group Access Identification	Check this check box to use the device ID for Security Group Access Identification. When you check this check box, the following field, Device ID, is disabled.
Device ID	Name that will be used for Security Group Access identification of this device. By default, you can use the configured device name. If you want to use another name, clear the Use device name for Security Group Access identification check box, and enter the name in the Identification field.
Password	Security Group Access authentication password.
Security Group Access Advanced Settings	Check to display additional Security Group Access fields.
Other Security Group Access devices to trust this device (SGA trusted)	Specifies whether all the device's peer devices trust this device. The default is checked, which means that the peer devices trust this device, and do not change the SGTs on packets arriving from this device. If you uncheck the check box, the peer devices repaint packets from this device with the related peer SGT.
Download peer authorization policy every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for the peer authorization policy. ACS returns this information to the device in the response to a peer policy request. The default is 1 day.
Download SGACL lists every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for SGACL lists. ACS returns this information to the device in the response to a request for SGACL lists. The default is 1 day.

Table 7-4 Creating Network Devices and AAA Clients (continued)

Option	Description
Download environment data every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for environment data. ACS returns this information to the device in the response to a request for environment data. The default is 1 day.
Re-authentication every: Weeks Days Hours Minutes Seconds	Specifies the dot1x (.1x) reauthentication period. ACS configures this for the supplicant and returns this information to the authenticator. The default is 1 day.

1. The Device Type and Location network device groups are predefined at installation. You can define an additional 10 network device groups. See [Creating, Duplicating, and Editing Network Device Groups, page 7-2](#) for information on how to define network device groups. If you have defined additional network device groups, they appear in alphabetical order in the Network Device Groups page and in the Network Resources drawer in the left navigation pane.

Displaying Network Device Properties

Choose **Network Resources > Network Devices and AAA Clients**, then click a device name or check the check box a device name, and click **Edit** or **Duplicate**.

The Network Devices and AAA Clients Properties page appears, displaying the information described in [Table 7-5](#):

Table 7-5 Network Devices and AAA Clients Properties Page

Option	Description
Name	Name of the network device. If you are duplicating a network device, you must enter a unique name as a minimum configuration; all other fields are optional.
Description	Description of the network device.
Network Device Groups¹	
Location: Select	Click Select to display the Network Device Groups selection box. Click the radio button the network device group you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
Device Type: Select	Click Select to display the Network Device Groups selection box. Click the radio button the device type network device group that you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
IP Address	
The IP addresses and subnet masks associated with the network device. Select to enter a single IP address or to define a range.	
Single IP Address	Choose to enter a single IP address. In ACS 5.8.1, you can configure a network device with a single static IP address that can be part of a IP subnet or range configured on another network device. For more information, see Using Single Static IP Addresses That Are Part of IP Subnets and IP Ranges, page 7-17

Table 7-5 Network Devices and AAA Clients Properties Page (continued)

Option	Description
IP Subnets	<p>Choose to enter an IP address range. You can configure up to 40 IP addresses or subnet masks for each network device. If you use a subnet mask in this field, all IP addresses within the specified subnet mask are permitted to access the network and are associated with the network device definition.</p> <p>When you use subnet masks, the number of unique IP addresses depends on the number of IP addresses available through the subnet mask. For example, a subnet mask of 255.255.255.0 means you have 256 unique IP addresses.</p> <p>The first six IP addresses appear in the field; use the scroll bar to see any additional configured IP addresses.</p> <p>A mask is needed only for wildcards—if you want an IP address range. You cannot use asterisk (*) as wildcards.</p>
IP Range(s)	<p>Choose to enter single or multiple ranges of IP address. You can configure up to 40 IP addresses or subnet masks for each network device. You can also exclude a subnet of IP address range from the configured range in a scenario where that subset has already been added.</p> <p>You can use a hyphen (-) to specify a range of IP address. You can also add IP addresses with wildcards. You can use asterisks (*) as wildcards.</p> <p>Some examples of entering IP address ranges are:</p> <ul style="list-style-type: none"> • A single range—10.77.10.1-10,,, 192.120.10-12.10 • Multiple ranges—10.*.1-20.10, 192.1-23.*.100-150 • Exclusions from a range—10.10.1-255.* exclude 10.10.10-200.100-150 <p>Using dynamic device IP address ranges (for example: 1-5.*.7.9) can have performance implications on both the run-time and the management.</p> <p>Therefore, we recommend using IP address and subnet mask whenever possible. The dynamic IP address ranges should be used only when the range cannot be described using IP address and subnet mask.</p>
Authentication Options	
TACACS+	<p>Check to use the Cisco IOS TACACS+ protocol to authenticate communication to and from the network device.</p> <p>You must use this option if the network device is a Cisco device-management application, such as Management Center for Firewalls. You should use this option when the network device is a Cisco access server, router, or firewall.</p>
TACACS+ Shared Secret	<p>Shared secret of the network device, if you enabled the TACACS+ protocol.</p> <p>A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.</p>
Single Connect Device	<p>Check to use a single TCP connection for all TACACS+ communication with the network device. Choose one:</p> <ul style="list-style-type: none"> • Legacy TACACS+ Single Connect Support • TACACS+ Draft Compliant Single Connect Support <p>If you disable this option, a new TCP connection is used for every TACACS+ request.</p>
RADIUS	Check to use the RADIUS protocol to authenticate communication to and from the network device.

Table 7-5 Network Devices and AAA Clients Properties Page (continued)

Option	Description
RADIUS Shared Secret	Shared secret of the network device, if you have enabled the RADIUS protocol. A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.
CoA Port	Used to set up the RADIUS CoA port for session directory, for user authentication. This session directory can be launched from Monitoring and Troubleshooting Viewer page. By default, the CoA port value is filled as 1700.
Enable KeyWrap	Check to enable the shared secret keys for RADIUS Key Wrap in PEAP, EAP-FAST and EAP-TLS authentications. Each key must be unique and be distinct from the RADIUS shared key. You can configure these shared keys for each AAA Client.
Key Encryption Key (KEK)	Used to encrypt the Pairwise Master Key (PMK). In ASCII mode, enter a key with 16 characters. In hexadecimal mode, enter a key with 32 characters.
Message Authentication Code Key (MACK)	Used to calculate the keyed hashed message authentication code (HMAC) over the RADIUS message. In ASCII mode, enter a key length with 20 characters. In hexadecimal mode, enter a key with 40 characters.
Key Input Format	Enter the keys as ASCII or hexadecimal strings. The default is hexadecimal.
Security Group Access	Appears only when you enable the Cisco Security Group Access feature. Check to use Security Group Access functionality on the network device. If the network device is the seed device (first device in the Security Group Access network), you must also check the RADIUS check box.
Identification	Name that will be used for Security Group Access identification of this device. By default, you can use the configured device name. If you want to use another name, clear the Use device name for Security Group Access identification check box, and enter the name in the Identification field.
Password	Security Group Access authentication password.
Security Group Access Advanced Settings	Check to display additional Security Group Access fields.
Other Security Group Access devices to trust this device	Specifies whether all the device's peer devices trust this device. The default is checked, which means that the peer devices trust this device, and do not change the SGTs on packets arriving from this device. If you uncheck the check box, the peer devices repaint packets from this device with the related peer SGT.
Download peer authorization policy every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for the peer authorization policy. ACS returns this information to the device in the response to a peer policy request. The default is 1 day.
Download SGACL lists every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for SGACL lists. ACS returns this information to the device in the response to a request for SGACL lists. The default is 1 day.

Table 7-5 Network Devices and AAA Clients Properties Page (continued)

Option	Description
Download environment data every: Weeks Days Hours Minutes Seconds	Specifies the expiry time for environment data. ACS returns this information to the device in the response to a request for environment data. The default is 1 day.
Re-authentication every: Weeks Days Hours Minutes Seconds	Specifies the dot1x (.1x) reauthentication period. ACS configures this for the supplicant and returns this information to the authenticator. The default is 1 day.

1. The Device Type and Location network device groups are predefined at installation. You can define an additional 10 network device groups. See [Creating, Duplicating, and Editing Network Device Groups, page 7-2](#), for information on how to define network device groups. If you have defined additional network device groups, they appear in the Network Device Groups page and in the Network Resources drawer in the left navigation pane, in alphabetical order.

Related Topics:

- [Viewing and Performing Bulk Operations for Network Devices, page 7-5](#)
- [Creating, Duplicating, and Editing Network Device Groups, page 7-2](#)

Deleting Network Devices

To delete a network device:

-
- | | |
|---------------|--|
| Step 1 | Choose Network Resources > Network Devices and AAA Clients .

The Network Devices page appears, with a list of your configured network devices. |
| Step 2 | Check one or more check boxes the network devices you want to delete. |
| Step 3 | Click Delete .

The following message appears:

<code>Are you sure you want to delete the selected item/items?</code> |
| Step 4 | Click OK .

The Network Devices page appears, without the deleted network devices listed. The network device is removed from the device repository. |
-

Using Single Static IP Addresses That Are Part of IP Subnets and IP Ranges

ACS 5.8.1 allows you to configure a network device with a single static IP address that can be part of an IP subnet or range configured on another network device.

For example, when you have network devices with the IP range 1.0-10.0-10.1 in ACS, the administrator can configure another network device with the IP address 1.1.1.1.

ACS allows you to use single static IPv4 or IPv6 addresses that are also a part of IP subnets and single static IPv4 addresses that are a part of IP ranges.

When ACS receives an access request, it searches the single static IP addresses first. If a match is not found, ACS searches the IP subnets and IP ranges for the network device. An IP address with a subnet mask of 32 resolves to the IP address itself. Therefore, ACS does not allow you to configure a single static IP address on a network device if the same IP address with a subnet mask of 32 is configured on another network device.

ACS displays all the occurrences of an IP address (Single IP address, IP subnet, and IP ranges) when you filter network devices on the Network Device and AAA Clients page.

Configuring a Default Network Device

While processing requests, ACS searches the network device repository for a network device whose IP address matches the IP address presented in the request. If the search does not yield a match, ACS uses the default network device definition for RADIUS or TACACS+ requests.

The default network device defines the shared secret to be used and also provides NDG definitions for RADIUS or TACACS+ requests that use the default network device definition.

Choose **Network Resources > Default Network Device** to configure the default network device. The Default Network Device page appears, displaying the information described in [Table 7-6 on page 18](#).

Table 7-6 *Default Network Device Page*

Option	Description
Default Network Device	
The default device definition can optionally be used in cases where no specific device definition is found that matches a device IP address.	
Default Network Device Status	Choose Enabled from the drop-down list box to move the default network device to the active state.
Network Device Groups	
Location	Click Select to display the Network Device Groups selection box. Click the radio button the Location network device group you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
Device Type	Click Select to display the Network Device Groups selection box. Click the radio button the Device Type network device group you want to associate with the network device. See Creating, Duplicating, and Editing Network Device Groups, page 7-2 for information about creating network device groups.
Authentication Options	
TACACS+	Check to use the Cisco IOS TACACS+ protocol to authenticate communication to and from the network device. You must use this option if the network device is a Cisco device-management application, such as Management Center for Firewalls. You should use this option when the network device is a Cisco access server, router, or firewall.

Table 7-6 Default Network Device Page (continued)

Option	Description
Shared Secret	<p>Shared secret of the network device, if you enabled the TACACS+ protocol.</p> <p>A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.</p>
Single Connect Device	<p>Check to use a single TCP connection for all TACACS+ communication with the network device. Choose one:</p> <ul style="list-style-type: none"> Legacy TACACS+ Single Connect Support TACACS+ Draft Compliant Single Connect Support <p>If you disable this option, ACS uses a new TCP connection for every TACACS+ request.</p>
RADIUS	Check to use the RADIUS protocol to authenticate communication to and from the network device.
Shared Secret	<p>Shared secret of the network device, if you have enabled the RADIUS protocol.</p> <p>A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.</p>
CoA Port	Used to set up the RADIUS CoA port for session directory, for user authentication. This session directory can be launched from Monitoring and Troubleshooting Viewer page. By default, the CoA port value is filled as 1700.
Enable KeyWrap	Check to enable the shared secret keys for RADIUS Key Wrap in PEAP, EAP-FAST and EAP-TLS authentications. Each key must be unique and be distinct from the RADIUS shared key. You can configure these shared keys for each AAA Client.
Key Encryption Key (KEK)	Used to encrypt the Pairwise Master Key (PMK). In ASCII mode, enter a key with 16 characters. In hexadecimal mode, enter a key with 32 characters.
Message Authentication Code Key (MACK)	<p>Used to calculate the keyed hashed message authentication code (HMAC) over the RADIUS message.</p> <p>In ASCII mode, enter a key length with 20 characters. In hexadecimal mode, enter a key with 40 characters.</p>
Key Input Format	Enter the keys as ASCII or hexadecimal strings. The default is hexadecimal.

Related Topics

- [Network Device Groups, page 7-1](#)
- [Network Devices and AAA Clients, page 7-5](#)
- [Creating, Duplicating, and Editing Network Device Groups, page 7-2](#)

Working with External Proxy Servers

ACS 5.8.1 can function both as a RADIUS and TACACS+ server and as a RADIUS and TACACS+ proxy server. When it acts as a proxy server, ACS receives authentication and accounting requests from the NAS and forwards them to the external RADIUS or TACACS+ server.

ACS accepts the results of the requests and returns them to the NAS. You must configure the external RADIUS or TACACS+ servers in ACS to enable ACS to forward requests to them. You can define the timeout period and the number of connection attempts.

ACS can simultaneously act as a proxy server to multiple external RADIUS or TACACS+ servers.

RADIUS proxy server can handle the looping scenario whereas TACACS+ proxy server cannot.

**Note**

You can use the external RADIUS or TACACS+ servers that you configure here in access services of the RADIUS or TACACS+ proxy service type.

This section contains the following topics:

- [Creating, Duplicating, and Editing External Proxy Servers, page 7-20](#)
- [Deleting External Proxy Servers, page 7-21](#)

Creating, Duplicating, and Editing External Proxy Servers

To create, duplicate, or edit an external proxy server:

-
- Step 1** Choose **Network Resources > External Proxy Servers**.
- The External Proxy Servers page appears with a list of configured servers.
- Step 2** Do one of the following:
- Click **Create**.
 - Check the check box the external proxy server that you want to duplicate, then click **Duplicate**.
 - Click the external proxy server name that you want to edit, or check the check box the name and click **Edit**.
- The External Proxy Servers page appears.
- Step 3** Edit fields in the External Proxy Servers page as shown in [Table 7-7 on page 20](#).

Table 7-7 *External Policy Servers Page*

Option	Description
General	
Name	Name of the external RADIUS or TACACS+ server.
Description	(Optional) The description of the external RADIUS or TACACS+ server.
Server Connection	
Server IP Address	IP address of the external RADIUS or TACACS+ server. It can be either an IPv4 or IPv6 address. ACS 5.8.1 validates the IP address, if the address is entered in the supported format. It displays an error message if the entered format is not correct.

Table 7-7 External Policy Servers Page

Option	Description
Shared Secret	<p>Shared secret between ACS and the external RADIUS or TACACS+ server that is used for authenticating the external RADIUS or TACACS+ server.</p> <p>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.</p> <p>Show/Hide button is available to view the Shared secret in plain text or hidden format.</p>
Advanced Options	
RADIUS	Choose to create a RADIUS proxy server. RADIUS supports only IPv4 addresses.
TACACS+	Choose to create a TACACS+ proxy server. TACACS+ supports IPv4 and IPv6 addresses.
Cisco Secure ACS	Default choice. Supports both RADIUS and TACACS+. You can choose Cisco Secure ACS if you use an IPv4 or IPv6 address.
Authentication Port	RADIUS authentication port number. The default is 1812.
Accounting Port	RADIUS accounting port number. The default is 1813.
Server Timeout	Number of seconds ACS waits for a response from the external RADIUS server. The default is 5 seconds. Valid values are from 1 to 300.
Connection Attempts	Number of times ACS attempts to connect to the external RADIUS server. The default is 3 attempts. Valid values are from 1 to 99.
Connection Port	TACACS+ connection port. The default is 49.
Network Timeout	Number of seconds ACS waits for a response from the external TACACS+ server. The default is 20 seconds.

Step 4 Click **Submit** to save the changes.

The external Proxy Server configuration is saved. The External Proxy Server page appears with the new configuration.



Note

If you want ACS to forward unknown RADIUS attributes you have to define VSAs for proxy.

Related Topics

- [RADIUS and TACACS+ Proxy Services, page 3-7](#)
- [RADIUS and TACACS+ Proxy Requests, page 4-27](#)
- [Configuring General Access Service Properties, page 10-13](#)
- [Deleting External Proxy Servers, page 7-21](#)

Deleting External Proxy Servers

To delete an external proxy server:

Step 1 Choose **Network Resources > External Proxy Servers**.

The External Proxy Servers page appears with a list of configured servers.

- Step 2** Check one or more check boxes the external RADIUS or TACACS+ servers you want to delete, and click **Delete**.

The following message appears:

Are you sure you want to delete the selected item/items?

- Step 3** Click **OK**.

The External Proxy Servers page appears without the deleted server(s).

Working with OSCP Services

ACS 5.8.1 introduces a new protocol, Online Certificate Status Protocol (OCSP), which is used to check the status of x.509 digital certificates. This protocol can be used as an alternate to the certificate revocation list (CRL). It can also address the issues that result when handling CRLs.

ACS 5.8.1 communicates with OSCP services over HTTP to validate the status of the certificates in authentications. OSCP is configured in a reusable configuration object, and OSCP can be referenced from any certificate authority (CA) certificate that is configured in ACS. Multiple CA objects can reference the same OSCP service.

You can configure up to two OSCP servers in ACS, which are called the primary and secondary OSCP servers. ACS communicates with the secondary OSCP server when a timeout occurs while it is communicating with the primary OSCP server.

OCSP can return the following three values for a given certificate request:

- Good—The certificate is good for usage.
- Revoked—The certificate is revoked.
- Unknown —The certificate status is unknown.

The status of the certificate is unknown if the OSCP is not configured to handle the given certificate CA. In this case, the certificate is handled as an unknown certificate; that is, the validation process checks the *Reject the request if no status* flag. If the flag is set in such a way that the request should not be rejected, then OSCP continues to CRL to check whether the certificate is configured in ACS.

ACS caches all OSCP responses. This is to maximize the performance and reduce the load in the OSCP servers. At the time of OSCP verification, ACS looks for the relevant information in the cache first. If the relevant information is not found, then ACS establishes a connection to the OSCP server. ACS defines a lifetime for all OSCP records in each OSCP service. In addition, each OSCP response has a Time to Live that defines the interval after which a new request should be made. Each cache entry is retained for either the Time to Live or the cache lifetime, whichever is shorter. Click **Clear Cache** to clear all the cached records that are associated with this OSCP service. Clear Cache also clears the records in the secondary ACS servers in a distributed system.

ACS does not support replicating the cached responses database. The caches are not persistent; therefore, the cached responses are cleared after you restart the ACS application.

ACS verifies the user certificates and the CA certificates and creates a set of logs for both the certificates in RADIUS Authentication reports page. Therefore, OSCP logs appear twice in the RADIUS Authentication reports page for the passed authentications whereas for the failed authentications, it appears only once.

The following logs are displayed twice when ACS communicates with the OSCP server for the first time:

- 12568 Lookup user certificate status in OCSP cache.
- 12569 User certificate status was not found in OCSP cache.
- 12550 Sent an OCSP request to the primary OCSP server for the CA.
- 12553 Received OCSP response.
- 12554 OCSP status of user certificate is good.

The following logs are displayed twice when ACS communicates searches the cached OCSP responses for the subsequent verifications based on either the cache Time to Live or the cache Lifetime options:

- 12568 Lookup user certificate status in OCSP cache.
- 12570 Lookup user certificate status in OCSP cache succeeded.
- 12554 OCSP status of user certificate is good.

This section contains the following topics:

- [Creating, Duplicating, and Editing OCSP Servers, page 7-23](#)
- [Deleting OCSP Servers, page 7-25](#)

Creating, Duplicating, and Editing OCSP Servers

To create, duplicate, or edit an OCSP server:

Step 1 Choose **Network Resources > OCSP Services**.

The OCSP Services page appears with a list of configured OCSP servers.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box the OCSP server that you want to duplicate, then click **Duplicate**.
- Click the OCSP server name that you want to edit, or check the check box the name and click **Edit**.

The OCSP Servers page appears.

Step 3 Edit fields in the OCSP Servers page as shown in [Table 7-8 on page 23](#).

Table 7-8 OCSP Servers Page

Option	Description
Name	Name of the OCSP server.
Description	(Optional) The description of the OCSP server.
Server Connection	
Enable Secondary Server	Check this check box to enable the secondary server configuration, such as Always Access Primary Server First and Failback options.
Always Access Primary Server First	Enable this option to check the primary server first before moving on to the secondary server, even if there was no previous response from the primary server.
Failback To Primary Server	Enable this option to use the secondary server for the given amount of time when the primary is completely down. The time range is 1 to 1440 minutes.
Primary Server	
URL	Enter the URL or the IP address of the primary server.

Table 7-8 OSCP Servers Page

Option	Description
Enable Nonce Extension Support	<p>Check this check box to use a nonce in the OSCP request.</p> <p>This option includes a random number in the OSCP request. When you select this option, it compares the number that is received in the response with the number that is included in the request. This method ensures that old communications are not reused.</p> <p>You can configure a nonce in Windows 2008 and 2012 servers. If the nonce from the ACS server is not matched with the Windows server, Windows returns an unauthorized response. As a result, ACS fails the request and considers this to be an unknown certificate.</p>
Validate Response Signature	<p>Check this check box to instruct the OSCP responder to include one of the following signatures in the response:</p> <ul style="list-style-type: none"> • The CA certificate • A different certificate from the CA certificate <p>ACS validates the response certificate based on the OSCP response signature. If there is no OSCP response signature, then ACS fails the response, and the status of the certificate cannot be determined.</p>
Network Timeout	Enter the number of seconds that ACS should wait for a response from the primary OSCP server. The default is 5 seconds. Valid values are from 1 to 300 seconds.
Secondary Server	
URL	Enter the URL or the IP address of the secondary server.
Enable Nonce Extension Support	<p>Check this check box to use a nonce in the OSCP request.</p> <p>This option includes a random number in the OSCP request. When you select this option, it compares the number that is received in the response with the number that is included in the request. This method ensures that old communications are not reused.</p> <p>You can configure a nonce in Windows 2008 and 2012 servers. If the nonce from the ACS server is not matched with the Windows server, Windows returns an unauthorized response. As a result, ACS fails the request and considers this to be an unknown certificate.</p>
Validate Response Signature	<p>Check this check box to instruct the OSCP responder to include one of the following signatures in the response:</p> <ul style="list-style-type: none"> • The CA certificate • A different certificate from the CA certificate <p>ACS validates the response certificate based on the OSCP response signature. If there is no OSCP response signature, then ACS fails the response, and the status of the certificate cannot be determined.</p>
Network Timeout	Enter the number of seconds that ACS should wait for a response from the primary OSCP server. The default is 5 seconds. Valid values are from 1 to 300.
Response Cache	
Cache Entry Time To Live	Defines the interval after which the a new OSCP request should be made. Enter the value in number of minutes. The default value is 300 minutes.
Clear Cache	<p>Clears the Cache of the selected OSCP service for all the associated Certificate Authorities.</p> <p>The Clear Cache option can interact with all the nodes that are associated with this OSCP service within a deployment. This option also shows the updated status when you select it.</p>

Step 4 Click **Submit** to save your changes.

The OCSP Server configuration is saved. The OCSP Server page appears with the new configuration.

Related Topics

- [Deleting OCSP Servers, page 7-25](#)

Deleting OCSP Servers

To delete an OCSP server, complete the following steps:

Step 1 Choose **Network Resources > OCSP Services**.

The OCSP Services page appears with a list of configured OCSP servers.

Step 2 Check one or more check boxes the OCSP servers you want to delete, and click **Delete**.

The following message appears:

Are you sure you want to delete the selected item/items?

Step 3 Click **OK**.

The OCSP Servers page appears without the deleted server(s).



Managing Users and Identity Stores

This chapter describes the following topics:

- [Overview, page 8-1](#)
- [Managing Internal Identity Stores, page 8-4](#)
- [Managing External Identity Stores, page 8-29](#)
- [Configuring CA Certificates, page 8-95](#)
- [Configuring Certificate Authentication Profiles, page 8-99](#)
- [Configuring Identity Store Sequences, page 8-101](#)

Overview

ACS manages your network devices and other ACS clients by using the ACS network resource repositories and identity stores. When a host connects to the network through ACS requesting access to a particular network resource, ACS authenticates the host and decides whether the host can communicate with the network resource.

To authenticate and authorize a user or host, ACS uses the user definitions in identity stores. There are two types of identity stores:

- **Internal**—Identity stores that ACS maintains locally (also called local stores) are called *internal identity stores*. For internal identity stores, ACS provides interfaces for you to configure and maintain user records.
- **External**—Identity stores that reside outside of ACS are called *external identity stores*. ACS requires configuration information to connect to these external identity stores to perform authentication and obtain user information.

In addition to authenticating users and hosts, most identity stores return attributes that are associated with the users and hosts. You can use these attributes in policy conditions while processing a request and can also populate the values returned for RADIUS attributes in authorization profiles.

Internal Identity Stores

ACS maintains different internal identity stores to maintain user and host records. For each identity store, you can define identity attributes associated with that particular store for which values are defined while creating the user or host records.

You can define these identity attributes as part of identity dictionaries under the System Administration section of the ACS application (**System Administration > Configuration > Dictionaries > Identity**).

Each internal user record includes a password, and you can define a second password as a TACACS+ enable password. You can configure the password stored within the internal user identity store to expire after a particular time period and thus force users to change their own passwords periodically.

Users can change their passwords over the RADIUS or TACACS+ protocols or use the UCP web service. Passwords must conform to the password complexity criteria that you define in ACS.

Internal user records consist of two component types: fixed and configurable.

Fixed components are:

- Name
- Description
- Password
- Enabled or disabled status
- Email Address
- Identity group to which users belong

Configurable components are:

- Enable password for TACACS+ authentication
- Sets of identity attributes that determine how the user definition is displayed and entered
- Disable Account if Date Exceeds
- Disable account after n successive failed attempts
- Enable Password Hash
- Password Never Expired/Disabled

Cisco recommends that you configure identity attributes before you create users. When identity attributes are configured:

- You can enter the corresponding values as part of a user definition.
- They are available for use in policy decisions when the user authenticates.
- They can be used to populate the values returned for RADIUS attributes in an authorization profile.

Internal user identity attributes are applied to the user for the duration of the user's session.

Internal identity stores contain the internal user attributes and credential information used to authenticate internal users.

Internal host records are similar to internal user records, except that they do not contain any password information. Hosts are identified by their MAC addresses. For information on managing internal identity stores, see [Managing Internal Identity Stores, page 8-4](#).

External Identity Stores

External identity stores are external databases on which ACS performs authentications for internal and external users. ACS 5.8.1 supports the following external identity stores:

- LDAP
- Active Directory

- RSA SecurID Token Server
- RADIUS Identity Server

External identity store user records include configuration parameters that are required to access the specific store. You can define attributes for user records in all the external identity stores except the RSA SecurID Token Server. External identity stores also include certificate information for the ACS server certificate and certificate authentication profiles.

For more information on how to manage external identity stores, see [Managing External Identity Stores, page 8-29](#).

Identity Stores with Two-Factor Authentication

You can use the RSA SecurID Token Server and RADIUS Identity Server to provide two-factor authentication. These external identity stores use an OTP that provides greater security. The following additional configuration options are available for these external identity stores:

- Identity caching—You can enable identity caching for ACS to use the identity store while processing a request in cases where authentication is not performed. Unlike LDAP and AD, for which you can perform a user lookup without user authentication, the RSA SecurID Token Server and RADIUS Identity Server does not support user lookup.

For example, in order to authorize a TACACS+ request separately from the authentication request, taking into account that it is not possible for the identity store to retrieve the data because authentication is not performed, you can enable identity caching to cache results and attributes retrieved from the last successful authentication for the user. You can use this cache to authorize the request.

- Treat authentication rejects as—The RSA and RADIUS identity stores do not differentiate between the following results when an authentication attempt is rejected:
 - Authentication Failed
 - User Not Found

This classification is very important when you determine the fail-open operation. A configuration option is available, allowing you to define which result must be used.

Identity Groups

Identity groups are logical entities that are defined within a hierarchy and are associated with users and hosts. These identity groups are used to make policy decisions. For internal users and hosts, the identity group is defined as part of the user or host definition.

When external identity stores are used, the group mapping policy is used to map attributes and groups retrieved from the external identity store to an ACS identity group. Identity groups are similar in concept to Active Directory groups but are more basic in nature.

Certificate-Based Authentication

Users and hosts can identify themselves with a certificate-based access request. To process this request, you must define a certificate authentication profile in the identity policy.

The certificate authentication profile includes the attribute from the certificate that is used to identify the user or host. It can also optionally include an LDAP or AD identity store that can be used to validate the certificate present in the request. For more information on certificates and certificate-based authentication, see:

- [Configuring CA Certificates, page 8-95](#)
- [Configuring Certificate Authentication Profiles, page 8-99](#)

Identity Sequences

You can configure a complex condition where multiple identity stores and profiles are used to process a request. You can define these identity methods in an Identity Sequence object. The identity methods within a sequence can be of any type.

The identity sequence is made up of two components, one for authentication and the other for retrieving attributes.

- If you choose to perform authentication based on a certificate, a single certificate authentication profile is used.
- If you choose to perform authentication on an identity database, you can define a list of identity databases to be accessed in sequence until the authentication succeeds. If the authentication succeeds, the attributes within the database are retrieved.

In addition, you can configure an optional list of databases from which additional attributes can be retrieved. These additional databases can be configured irrespective of whether you use password-based or certificate-based authentication.

If a certificate-based authentication is performed, the username is populated from a certificate attribute and this username is used to retrieve attributes from all the databases in the list. For more information on certificate attributes, see [Configuring CA Certificates, page 8-95](#).

When a matching record is found for the user, the corresponding attributes are retrieved. ACS retrieves attributes even for users whose accounts are disabled or whose passwords are marked for change.



Note

An internal user account that is disabled is available as a source for attributes, but not for authentication.

For more information on identity sequences, see [Configuring Identity Store Sequences, page 8-101](#).

This chapter contains the following sections:

- [Managing Internal Identity Stores, page 8-4](#)
- [Managing External Identity Stores, page 8-29](#)
- [Configuring CA Certificates, page 8-95](#)
- [Configuring Certificate Authentication Profiles, page 8-99](#)
- [Configuring Identity Store Sequences, page 8-101](#)

Managing Internal Identity Stores

ACS contains an identity store for users and an identity store for hosts:

- The internal identity store for *users* is a repository of users, user attributes, and user authentication options.

- The internal identity store for *hosts* contains information about hosts for MAC Authentication Bypass (Host Lookup).

You can define each user and host in the identity stores, and you can import files of users and hosts.

The identity store for users is shared across all ACS instances in a deployment and includes for each user:

- Standard attributes
- User attributes
- Authentication information



Note

ACS 5.8.1 supports authentication for internal users against the internal identity store only.

This section contains the following topics:

- [Authentication Information, page 8-5](#)
- [Identity Groups, page 8-6](#)
- [Managing Identity Attributes, page 8-7](#)
- [Configuring Authentication Settings for Users, page 8-9](#)
- [Disabling User Account After N Days of Inactivity, page 8-12](#)
- [Creating Internal Users, page 8-13](#)
- [Enable and Disable Password Hashing for Internal Users, page 8-18](#)
- [Configuring Password Expiry Notification Emails to Users and Administrators, page 8-19](#)
- [Viewing and Performing Bulk Operations for Internal Identity Store Users, page 8-21](#)
- [Configuring Authentication Settings for Hosts, page 8-22](#)
- [Creating Hosts in Identity Stores, page 8-23](#)
- [Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-25](#)
- [Management Hierarchy, page 8-26](#)

Authentication Information

You can configure an additional password, stored as part of the internal user record that defines the user's TACACS+ enable password which sets the access level to device. If you do not select this option, the standard user password is also used for TACACS+ enable.

If the system is not being used for TACACS+ enable operations, you should not select this option.

To use the identity store sequence feature, you define the list of identity stores to be accessed in a sequence. You can include the same identity store in authentication and attribute retrieval sequence lists; however, if an identity store is used for authentication, it is not accessed for additional attribute retrieval.

For certificate-based authentication, the username is populated from the certificate attribute and is used for attribute retrieval.

During the authentication process, authentication fails if more than one instance of a user or host exists in internal identity stores. Attributes are retrieved (but authentication is denied) for users who have disabled accounts or passwords that must be changed.

These types of failures can occur while processing the identity policy:

- Authentication failure; possible causes include bad credentials, disabled user, and so on.

- User or host does not exist in any of the authentication databases.
- Failure occurred while accessing the defined databases.

You can define fail-open options to determine what actions to take when each of these failures occurs:

- **Reject**—Send a reject reply.
- **Drop**—Do not send a reply.
- **Continue**—Continue processing to the next defined policy in the service.

The system attribute, *AuthenticationStatus*, retains the result of the identity policy processing. If you choose to continue policy processing when a failure occurs, you can use this attribute in a condition in subsequent policy processing to distinguish cases where identity policy processing did not succeed.

You can continue processing when authentication fails for PAP/ASCII, EAP-TLS, or EAP-MD5. For all other authentication protocols, the request is rejected and a message to this effect is logged.

Identity Groups

You can assign each internal user to one identity group. Identity groups are defined within a hierarchical structure. They are logical entities that are associated with users, but do not contain data or attributes other than the name you give to them.

You use identity groups within policy conditions to create logical groups of users to which the same policy results are applied. You can associate each user in the internal identity store with a single identity group.

When ACS processes a request for a user, the identity group for the user is retrieved and can then be used in conditions in the rule table. Identity groups are hierarchical in structure.

You can map identity groups and users in external identity stores to ACS identity groups by using a group mapping policy.

Creating Identity Groups

To create an identity group:

Step 1 Choose **Users and Identity Stores > Identity Groups**.

The Identity Groups page appears.

Step 2 Click **Create**. You can also:

- Check the check box next to the identity group that you want to duplicate, then click **Duplicate**.
- Click the identity group name that you want to modify, or check the check box next to the name and click **Edit**.
- Click **File Operations** to:
 - **Add**—Adds identity groups from the import to ACS.
 - **Update**—Overwrites the existing identity groups in ACS with the list from the import.
 - **Delete**—Removes the identity groups listed in the import from ACS.
- Click **Export** to export a list of identity groups to your local hard disk.

For more information on the File Operations option, see [Performing Bulk Operations for Network Resources and Users](#), page 7-8.

The Create page or the Edit page appears when you choose the Create, Duplicate, or Edit option.

Step 3 Enter information in the following fields:

- **Name**—Enter a name for the identity group. If you are duplicating an identity group, you must enter a unique name; all other fields are optional.
- **Description**—Enter a description for the identity group.
- **Parent**—Click **Select** to select a network device group parent for the identity group.

Step 4 Click **Submit** to save changes.

The identity group configuration is saved. The Identity Groups page appears with the new configuration. If you created a new identity group, it is located within the hierarchy of the page beneath your parent identity group selection.

Related Topics

- [Managing Users and Identity Stores, page 8-1](#)
- [Managing Internal Identity Stores, page 8-4](#)
- [Performing Bulk Operations for Network Resources and Users, page 7-8](#)
- [Identity Groups, page 8-3](#)
- [Creating Identity Groups, page 8-6](#)
- [Deleting an Identity Group, page 8-7](#)

Deleting an Identity Group

To delete an identity group:

Step 1 Choose **Users and Identity Stores > Identity Groups**.

The Identity Groups page appears.

Step 2 Check one or more check boxes next to the identity groups you want to delete and click **Delete**.

The following error message appears:

Are you sure you want to delete the selected item/items?

Step 3 Click **OK**.

The Identity Groups page appears without the deleted identity groups.

Related Topic

- [Managing Identity Attributes, page 8-7](#)

Managing Identity Attributes

Administrators can define sets of identity attributes that become elements in policy conditions. For information about the ACS 5.8.1 policy model, see [ACS 5.x Policy Model, page 3-1](#). During authentication, identity attributes are taken from the internal data store when they are part of a policy condition.

ACS 5.8.1 interacts with identity elements to authenticate users and obtain attributes for input to an ACS policy.

Attribute definitions include the associated data type and valid values. The set of values depends on the type. For example, if the type is *integer*, the definition includes the valid range. ACS 5.8.1 provides a default value definition that can be used in the absence of an attribute value. The default value ensures that all attributes have at least one value.

Related Topics

- [Standard Attributes, page 8-8](#)
- [User Attributes, page 8-8](#)
- [Host Attributes, page 8-9](#)

Standard Attributes

[Table 8-1](#) describes the standard attributes in the internal user record.

Table 8-1 *Standard Attributes*

Attribute	Description
Username	ACS compares the username against the username in the authentication request. The comparison is case-insensitive.
Status	<ul style="list-style-type: none">• Enabled status indicates that the account is active.• Disabled status indicates that authentications for the username will fail.
Description	Text description of the attribute.
Identity Group	ACS associates each user to an identity group. See Managing Identity Attributes, page 8-7 for information.

User Attributes

Administrators can create and add user-defined attributes from the set of identity attributes. You can then assign default values for these attributes for each user in the internal identity store and define whether the default values are required or optional.

You need to define users in ACS, which includes associating each internal user with an identity group, a description (optional), a password, an enable password (optional), and internal and external user attributes.

Internal users are defined by two components: fixed and configurable. Fixed components consist of these attributes:

- Name
- Description
- Password
- Enabled or disabled status
- Identity group to which they belong

Configurable components consist of these attributes:

- Enable password for TACACS+ authentication

- Sets of identity attributes that determine how the user definition is displayed and entered

Cisco recommends that you configure identity attributes before you create users. When identity attributes are configured:

- You can enter the corresponding values as part of a user definition.
- They are available for use in policy decisions when the user authenticates.

Internal user identity attributes are applied to the user for the duration of the user's session.

Internal identity stores contain the internal user attributes and credential information used to authenticate internal users (as defined by you within a policy).

External identity stores are external databases on which to perform credential and authentication validations for internal and external users (as defined by you within a policy).

In ACS 5.8.1, you can configure identity attributes that are used within your policies, in this order:

-
- | | |
|---------------|---|
| Step 1 | Define an identity attribute (using the user dictionary). |
| Step 2 | Define custom conditions to be used in a policy. |
| Step 3 | Populate values for each user in the internal database. |
| Step 4 | Define rules based on this condition. |
-

As you become more familiar with ACS 5.8.1 and your identity attributes for users, the policies themselves will become more robust and complex.

You can use the user-defined attribute values to manage policies and authorization profiles. See [Creating, Duplicating, and Editing an Internal User Identity Attribute, page 18-12](#) for information on how to create a user attribute.

Host Attributes

You can configure additional attributes for internal hosts. You can do the following when you create an internal host:

- Create host attributes
- Assign default values to the host attributes
- Define whether the default values are required or optional

You can enter values for these host attributes and can use these values to manage policies and authorization profiles. See [Creating, Duplicating, and Editing an Internal Host Identity Attribute, page 18-14](#) for information on how to create a host attribute.

Configuring Authentication Settings for Users

You can configure the authentication settings for user accounts in ACS to force users to use strong passwords. Any password policy changes that you make in the Authentication Settings page apply to all internal identity store user accounts. The User Authentication Settings page consists of the following tabs:

- Password complexity
- Advanced

To configure a password policy:

- Step 1** Choose **System Administration > Users > Authentication Settings**.
- The User Authentication Settings page appears with the Password Complexity and **Advanced** tabs.
- Step 2** In the **Password Complexity** tab, check each check box that you want to use to configure your user password.

[Table 8-2](#) describes the fields in the Password Complexity tab.

Table 8-2 Password Complexity Tab

Option	Description
Applies to all ACS internal identity store user accounts	
Minimum length	Required minimum length; the valid options are 4 to 32.
Password may not contain the username	Whether the password may contain the username or reverse username.
Password may not contain 'cisco'	Check to specify that the password cannot contain the word <i>cisco</i> .
Password may not contain	Check to specify that the password does not contain the string that you enter.
Password may not contain repeated characters four or more times consecutively	Check to specify that the password cannot repeat characters four or more times consecutively.
Change password failed reason message (for TACACS+ only)	Enter the error message that is displayed when a user enters a password that does not meet the password policy while trying to change the existing password. This option is applicable only for internal user TACACS+ authentication. The maximum length of this field is 50 characters. Using this option, you can display an appropriate error message for the internal users if their new password does not match the criteria that you have specified.
Password must contain at least one character of each of the selected types	
Lowercase alphabetic characters	Password must contain at least one lowercase alphabetic character.
Uppercase alphabetic characters	Password must contain at least one uppercase alphabetic character.
Numeric characters	Password must contain at least one numeric character.
Non-alphanumeric characters	Password must contain at least one non-alphanumeric character.

- Step 3** In the **Advanced** tab, enter the values for the criteria that you want to configure for your user authentication process. The following table describes the fields in the **Advanced** tab.

Table 8-3 Advanced Tab

Options	Description
Account Disable	
Supports account disablement policy for internal users.	
Never	Default option where accounts never expire. All internal users who got disabled because of this policy, are enabled if you select this option.

Table 8-3 Advanced Tab

Options	Description
Disable account if Date exceeds	<p>Internal user is disabled when the configured date exceeds. For example, if the configured date is 28th Dec 2010, all internal users will be disabled on the midnight of 28th Dec, 2010.</p> <p>The configured date can either be the current system date or a future date. You are not allowed to enter a date that is earlier than the current system date.</p> <p>All the internal users who get disabled due to Date exceeds option are enabled according to the configuration changes made in the Date exceeds option.</p>
Disable account if Days exceed	Internal user is disabled when the configured number of days exceed. For example, if the configured number of days to disable the account of a user is 60 days, that particular user will be disabled after 60 days from the time account was enabled.
Disable account if Failed Attempts Exceed	Internal user is disabled when the successive failed attempts count reaches the configured value. For example, if the configured value is 5, the internal user will be disabled when the successive failed attempts count reaches 5.
Reset current failed attempts count on submit	<p>If selected, failed attempts counts of all the internal users is set to 0.</p> <p>All internal users who were disabled because of Failed Attempts Exceed option are enabled.</p>
Disable user account after n days of inactivity	Specifies that the user account must be disabled based on the number of days the user is not logged in to the network. This option is applicable only for the internal users. The days ranges between 1 and 365.
Password History	
Password must be different from the previous n versions.	Specifies the number of previous passwords for this user to be compared against. The number of previous passwords include the default password as well. This option prevents the users from setting a password that was recently used. Valid options are 1 to 99.
Password Lifetime	
Users can be required to periodically change password	
Disable user account after n days if password is not changed for n days	Specifies that the user account must be disabled after n days if the password is not changed; the valid options are 1 to 365. This option is applicable only for TACACS+ and RADIUS with MS-CHAPv2 authentication.
Expire the password after n days if the password is not changed for n days	Specifies that the user password must be expired after n days if the password is not changed; valid options are 1 to 365. This option is applicable only for TACACS+ and RADIUS with MS-CHAPv2 authentication.
Display reminder after n days	Displays a reminder after n days to change password; the valid options are 1 to 365. This option, when set, only displays a reminder. It does not prompt you for a new password. This option is applicable only for TACACS+ and RADIUS with MS-CHAPv2 authentication.

Table 8-3 Advanced Tab

Options	Description
Send Email for password expiry before <i>n</i> days	Check this check box and enter the number of days if you want ACS to send an email notification a day to the internal users starting from <i>n</i> th day before their password expires. This option helps the internal users change their password before it expires. ACS does not allow you to configure this option without configuring the “Expire the password after <i>n</i> days if the password is not changed for <i>n</i> days” or “Disable user account after <i>n</i> days if password is not changed for <i>n</i> days options.”
TACACS Enable Password	
Select whether a separate password should be defined in the user record to store the Enable Password	
TACACS Enable Password	Check the check box to enable a separate password for TACACS+ authentication.

Step 4 Click **Submit**.

The user password is configured with the defined criteria. These criteria will apply only for future logins.

**Note**

If one of the users gets disabled, the failed attempt count value needs to be reconfigured multiple times. In such a case, the administrators should either note separately the current failed attempt count of that user, or reset the count to 0 for all users.

Disabling User Account After *N* Days of Inactivity

Before you Begin:

- This feature is applicable only for the ACS internal users.
- ACS must be configured to send passed authentication messages to the log collector server.
- The log collector server must be running and receiving syslog messages from all ACS nodes in the deployment.
- The log recovery feature must be enabled.

ACS 5.8.1 allows the administrator to configure the maximum number of days from ACS web interface during which the internal users' accounts are enabled despite the users not having logged in to the network. Once the configured period is exceeded, the user's account is disabled if the user has not logged in to the network. The number of days ranges between 1 and 365. For this feature to work properly, the log collector server should be running and receiving the syslog messages from ACS nodes in the deployment. The last login date is not stored in the database and hence it will not be displayed in the web interface. Every day at 10 PM, ACS View runs a job to provide the list of active users to the primary management. The active user is one who has made at least one successful authentication for the configured period of time. You can view the last active date of an user from the passed authentication reports in ACS Reports web interface. Based on this list, the primary management identifies the inactive users list, disables them, and sends an audit log message to the log collector server. The administrator can enable the disabled user account. After enabling the user account, the subsequent calculation for inactivity will be calculated from the last enabled date.

**Note**

When you change the log collector server, it is mandatory to restore the back up taken from the old log collector server in the new log collector server.

**Note**

When you restore the ACS backup from one ACS instance to another ACS instance, the view back up also should be restored along with the ACS backup.

To disable user accounts after n days of inactivity:

-
- Step 1** Choose **System Administration > Users > Authentication Settings**.
The User Authentication Settings page appears.
- Step 2** Check **Disable user account after n days of inactivity** check box.
- Step 3** Enter the number of days in the text box.
ACS disables the user account if it is not active for the configured number of days.
-

Creating Internal Users

In ACS, you can create internal users that do not access external identity stores for security reasons.

You can use the bulk import feature to import hundreds of internal users at a time; see [Performing Bulk Operations for Network Resources and Users, page 7-8](#) for more information. Alternatively, you can use the procedure described in this topic to create internal users one at a time.

-
- Step 1** Choose **Users and Identity Stores > Internal Identity Store > Users**.
The Internal Users page appears.
- Step 2** Click **Create**. You can also:
- Check the check box next to the user that you want to duplicate, then click **Duplicate**.
 - Click the username that you want to modify, or check the check box next to the name and click **Edit**.
 - Check the check box next to the user whose password you want to change, then click **Change Password**. You can also change internal user password using REST API. See [Changing internal user passwords using REST API](#) for more information.
- The Change Password page appears.
- Step 3** Complete the fields as described in [Table 8-4](#) to change the internal user password.

Table 8-4 Internal User - Change Password Page

Option	Description
Password Information	
Password Type	<p>Displays all configured external identity store names, along with Internal Users which is the default password type. You can choose any one identity store from the list.</p> <p>During user authentication, if an external identity store is configured for the user then internal identity store forwards the authentication request to the configured external identity store.</p> <p>If an external identity store is selected, you cannot configure a password for the user. The password edit box is disabled.</p> <p>You cannot use identity sequences as external identity stores for the Password Type.</p> <p>You can change Password Type using the Change Password button located in the Users and Identity Stores > Internal Identity Stores > Users page.</p>
Password	User's current password, which must comply with the password policies defined under System Administration > Users > Authentication Settings . The valid range is 4 to 32 characters.
Confirm Password	User's password, which must match the Password entry exactly.
Change Password on Next Login	Check this box to start the process to change the user's password at the next user login, after authentication with the old password.
Enable Password Information	
Enable Password	(Optional) The internal user's TACACS+ enable password, from 4 to 128 characters. You can disable this option. See Authentication Information, page 8-5 for more information.
Confirm Password	(Optional) The internal user's TACACS+ enable password, which must match the Enable Password entry exactly.

- Click **File Operations** to:
 - Add—Adds internal users from the import to ACS.
 - Update—Overwrites the existing internal users in ACS with the list of users from the import.
 - Delete—Removes the internal users listed in the import from ACS.
- Click **Export** to export a list of internal users to your local hard disk.

For more information on the File Operations option, see [Performing Bulk Operations for Network Resources and Users, page 7-8](#).

The User Properties page appears when you choose the Create, Duplicate, or Edit option. In the Edit view, you can see the information on the original creation and last modification of the user. You cannot edit this information.

Step 4 Complete the fields as described in [Table 8-5](#).

Table 8-5 *Users and Identity Stores > Internal Identity Store > User Properties Page*

Option	Description
General	
Name	Username.
Status	Use the drop-down list box to select the status for the user: <ul style="list-style-type: none"> • Enabled—Authentication requests for this user are allowed. • Disabled—Authentication requests for this user fail.
Description	(Optional) Description of the user.
Identity Group	Click Select to display the Identity Groups window. Choose an identity group and click OK to configure the user with a specific identity group.
Email Address	Enter the internal user email address. ACS View sends alerts to this email address. ACS uses this email address to notify the internal users about their password expiry <i>n</i> days before their password expires.
Account Disable	
Disable Account if Date Exceeds	Check this check box to use the account disablement policy for each individual user. This option allows you to disable the user accounts when the configured date is exceeded. This option overrides the global account disablement policy of the users. This means that the administrator can configure different expiry dates for different users as required. The default value for this option is 60 days from the account creation date. The user account will be disabled at midnight on the configured date.
Disable account after <i>n</i> successive failed attempts	Check this check box to configure the failed attempts count for each user. You can enter the failed attempts count at the text box provided. The value ranges from 1 to 99. If a user enters an incorrect login credentials, ACS uses this failed attempts count to decide whether it has to disable the user account or allow the user to try again. If the failed attempts count reaches <i>n</i> , then ACS disables the user account. If you do not configure the failed attempt count here, ACS tries to check the failed attempt count configuration at identity group level. The user level failed attempt count takes the precedence.
Password Hash	
Enable Password Hash	Check this check box to enable password hashing using the PBKDF2 of Cisco SSL hashing algorithm to provide enhanced security to the user passwords. This option is only applicable for internal users. If you enable this option, the authentication types such as CHAP and MSCHAP will not work. This option is disabled by default. When you disable this option in the middle, you have to re-configure your password using the change password option immediately after disabling this option. For more information, see Enable and Disable Password Hashing for Internal Users , page 8-18.
Password Lifetime	
Password Never Expired/Disabled	Check the Password Never Expired/Disabled check box for the user account to be active when the password lifetime is completed. This option overrides the password lifetime settings configured on the System Administration > Users > Authentication Settings > Advanced page.

Password Information

This section of the page appears only when you create an internal user.

Password must contain at least 4 characters

Table 8-5 *Users and Identity Stores > Internal Identity Store > User Properties Page (continued)*

Option	Description
Password Type	<p>Displays all configured external identity store names, along with Internal Users which is the default password type. You can choose any one identity store from the list.</p> <p>During user authentication, if an external identity store is configured for the user then internal identity store forwards the authentication request to the configured external identity store.</p> <p>If an external identity store is selected, you cannot configure a password for the user. The password edit box is disabled.</p> <p>You cannot use identity sequences as external identity stores for the Password Type.</p> <p>You can change Password Type using the Change Password button located in the Users and Identity Stores > Internal Identity Stores > Users page.</p>
Password	User's password, which must comply with the password policies defined under System Administration > Users > Authentication Settings .
Confirm Password	User's password, which must match the Password entry exactly.
Change Password on next login	Check this box to start the process to change the user's password when the user logs in next time, after authentication with the old password.

Enable Password Information

This section of the page appears only when you create an internal user.

Password must contain 4-128 characters.

Enable Password	(Optional) Internal user's TACACS+ enable password, from 4 to 128 characters. You can disable this option. See Authentication Information, page 8-5 for more information.
Confirm Password	(Optional) Internal user's TACACS+ enable password, which must match the Enable Password entry exactly.

User Information

If defined, this section displays additional identity attributes defined for user records.

ManagementHierarchy	<p>User's assigned access level of hierarchy. Enter the hierarchical level of the network devices that the user can access.</p> <p>Example:</p> <ul style="list-style-type: none"> Location:All:US:NY:MyMgmtCenter1 Location:All:US:NY:MyMgmtCenter1 US:NY:MyMgmtCenter2 <p>The attribute type is string and the maximum character length is 256.</p>
---------------------	---

Creation/Modification Information

This section of the page appears only after you have created or modified an internal user.

Table 8-5 Users and Identity Stores > Internal Identity Store > User Properties Page (continued)

Option	Description
Date Created	<p><i>Display only.</i> The date and time when the user's account was created, in the format <i>Day Mon dd hh:mm:ss UTC YYYY</i>, where:</p> <ul style="list-style-type: none"> <i>Day</i> = Day of the week. <i>Mon</i> = Three characters that represent the month of the year: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sept, Oct, Nov, Dec <i>DD</i> = Two digits that represent the day of the month; a space precedes single-digit days (1 to 9). <i>hh:mm:ss</i> = Hour, minute, and second, respectively <i>YYYY</i> = Four digits that represent the year
Date Modified	<p><i>Display only.</i> The date and time when the user's account was last modified (updated), in the format <i>Day Mon dd hh:mm:ss UTC YYYY</i>, where:</p> <ul style="list-style-type: none"> <i>Day</i> = Day of the week. <i>Mon</i> = Three characters that represent the month of the year: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sept, Oct, Nov, Dec <i>DD</i> = Two digits that represent the day of the month; a space precedes single-digit days (1 to 9). <i>hh:mm:ss</i> = Hour, minute, and second, respectively <i>YYYY</i> = Four digits that represent the year

Step 5 Click **Submit**.

The user configuration is saved. The Internal Users page appears with the new configuration.

**Note**

The **Password Never Expired/Disabled** option on the Creating Internal Users page overrides only the password lifetime settings configured on the **System Administration > Users > Authentication Settings > Advanced** page. This option does not override the account disablement settings due to date exceeds, days exceeds, failed attempt count exceeds, or n days of account inactivity.

Related Topics

- [Configuring Authentication Settings for Users, page 8-9](#)
- [Viewing and Performing Bulk Operations for Internal Identity Store Users, page 8-21](#)
- [Deleting Users from Internal Identity Stores, page 8-17](#)

Deleting Users from Internal Identity Stores

To delete a user from an internal identity store:

Step 1 Choose **Users and Identity Stores > Internal Identity Store > Users**.

The Internal Users page appears.

Step 2 Check one or more check boxes next to the users you want to delete.

Step 3 Click **Delete**.

The following message appears:

Are you sure you want to delete the selected item/items?

Step 4 Click **OK**.

The selected internal users are deleted.

Related Topics

- [Viewing and Performing Bulk Operations for Internal Identity Store Users, page 8-21](#)
- [Creating Internal Users, page 8-13](#)

Enable and Disable Password Hashing for Internal Users

ACS 5.8.1 provides enhanced security to the internal users' password by introducing the "Enable Password Hash" option in Creating Internal Users page of ACS web interface. Prior to Release 5.8.1, ACS stored the internal users' password as clear text in the ACS internal user database. The ACS administrators can view the internal users' passwords from internal user database. Therefore, to enhance security of internal users' password, ACS 5.8.1 introduces the new feature "Enable Password Hash". If you enable this option, the users' password is converted into hashes using the PBKDF2 of Cisco SSL hashing algorithm and is stored in the internal user database as hashes. This feature is applicable only for password based authentications. Therefore, when this option is enabled, you cannot use CHAP and MSCHAP authentications. If you enable this option while creating internal users, ACS converts the passwords to hashes and stores the same in the internal user database. When a user tries to access the network using the login password, ACS converts that password to hashes using the PBKDF2 hashing algorithm and compares this hash entry with the entry that is stored in ACS internal user's database. If the password hash value matches with the database hash value, then ACS allows the user to log in to the network. If the password hash value does not match with the database hash value, then ACS fails the authentication and the user cannot log in to the network. You can uncheck the Enable Password Hash check box to disable this option. Due to the iterations used in PDKDF2 algorithm to ensure stronger security, you can expect a delay in authentication response from ACS when there is a huge load on the server.

To enable password hashing for internal users in ACS:

Step 1 Choose **Users and Identity Stores > Internal Identity Stores > Users**.

The Internal Users page appears with the list of available internal users.

Step 2 Perform one of the following:

- Click **Create**.
- Check the check box next to the user to whom you want to enable password hash and click **Edit**.

Step 3 Check the **Enable Password Hash** check box.

Step 4 Click **Submit**.

The Password hashing option is enabled for the selected internal user.

To disable password hashing for internal users in ACS:

-
- Step 1** Choose **Users and Identity Stores > Internal Identity Stores > Users**.
The Internal Users page appears with the list of available internal users.
- Step 2** Check the check box next to the user to whom you want to disable password hash and click **Edit**.
- Step 3** Uncheck the **Enable Password Hash** check box.
- Step 4** Click **Submit**.

The Password hashing option is disabled for the selected internal user.



Note After disabling the **Enable Password Hash** option, you must change the user password immediately.

- Step 5** Check the check box next to the user to whom you have disabled the password hash option and click **Change Password**.
- Step 6** Enter the new password in the **Password** field.
- Step 7** Enter the new password in the **Confirm Password** field.
- Step 8** Click **Submit**.
-

Configuring Password Expiry Notification Emails to Users and Administrators

Before you Begin

- Email Settings must be configured under Monitoring Configuration. See [Specifying E Mail Settings, page 15-16](#) for Email Settings.

ACS 5.8.1 allows you to configure password expiry notification email for internal users and administrators. You can configure the number of days before the password expiry notification email must be sent for internal users and administrators from Creating Internal Users page from ACS web interface. If you configure this feature, then ACS 5.8.1 notifies the internal users and administrators through an email a day starting from *nth* day before their password expires. ACS verifies the users' and administrators' password expiry immediately after 5 minutes of the management process being restarted. The subsequent verifications are performed every 24 hours from the last verified time. For this feature to work properly, the **Email Settings** option must be configured under Monitoring Configuration.

Configuring Password Expiry Reminder for Users

To send password expiry reminder email to internal users, you have to configure the following from ACS web interface.

-
- Step 1** Choose **Users and Identity Stores > Internal Identity Stores > Users**.
The Internal Users page appears with the list of available internal users.
- Step 2** Perform one of the following:

- Click **Create**.
- Check the check box next to the user to whom you want to configure the password expiry reminder and click **Edit**.

Step 3 Enter the users' email address in the **Email Address** text box.

Step 4 Click **Submit**.

Step 5 Choose **System Administration > Users > Authentication Settings > Advanced**.

The Advanced Authentication Settings page for users appear.

Step 6 Check the **Send Email for password expiry before *n* days** check box and enter the number of days.



Note The **Send Email for password expiry before *n* days** check box is disabled if the password lifetime is not configured.

Step 7 Click **Submit**.

The password expiry reminder is configured now. The users will receive an email a day starting from the *n*th day before their password expires. The email has the following message:

Dear User,

Your password is going to expire on *day, date month year* at *time* UTC. We recommend that you reset your password immediately to avoid being locked out.

Regards,

CiscoSecureACS Administrator.

Configuring Password Expiry Reminder for Administrators

To send password expiry reminder email to internal administrators, you have to configure the following from ACS web interface.

Step 1 Choose **System Administration > Administrators > Accounts**.

The Administrators accounts page appear with the list of available internal administrators.

Step 2 Perform one of the following:

- Click **Create**.
- Check the check box next to the administrator to whom you want to configure the password expiry reminder and click **Edit**.

Step 3 Enter the administrators' email address in the **Email Address** text box.

Step 4 Click **Submit**.

Step 5 Choose **System Administration > Administrators > Settings > Authentication > Advanced**.

The Advanced Authentication Settings page for administrators appear.

Step 6 Check the **Send Email for password expiry before *n* days** check box and enter the number of days.



Note The **Send Email for password expiry before *n* days** check box is disabled if the **Disable administrator account after *n* days if password was not changed** option is not configured.

Step 7 Click Submit.

The password expiry reminder is configured now. The administrators will receive an email a day starting from the *n*th day before their password expires. The email has the following message:

Dear Administrator,

Your password is going to expire on *day, date month year* at *time* UTC. We recommend that you reset your password immediately to avoid being locked out.

Regards,

CiscoSecureACS Administrator.

Related Topics

- [Viewing and Performing Bulk Operations for Internal Identity Store Users, page 8-21](#)
- [Creating Internal Users, page 8-13](#)

Viewing and Performing Bulk Operations for Internal Identity Store Users

To view and perform bulk operations to internal identity store users:

Step 1 Choose Users and Identity Stores > Internal Identity Stores > Users.

The Internal Users page appears, with the following information for all configured users:

- Status—The status of the user
- User Name—The username of the user
- Identity Group—The identity group to which the user belongs
- Description—(Optional) A description of the user.

Step 2 Do one of the following:

- Click **Create**. For more information on creating internal users, see [Creating Internal Users, page 8-13](#).
- Check the check box next to an internal user whose information you want to edit and click **Edit**. For more information on the various fields in the edit internal user page, see [Creating Internal Users, page 8-13](#).
- Check the check box next to an internal user whose information you want to duplicate and click **Duplicate**. For more information on the various fields in the duplicate internal user page, see [Creating Internal Users, page 8-13](#).
- Click **File Operations** to perform any of the following bulk operations:
 - Add—Choose this option to add internal users from the import file to ACS.
 - Update—Choose this option to replace the list of internal users in ACS with the list of internal users in the import file.
 - Delete—Choose this option to delete the internal users listed in the import file from ACS.

See [Performing Bulk Operations for Network Resources and Users, page 7-8](#) for a detailed description of the bulk operations.

Related Topics

- [Creating Internal Users, page 8-13](#)
- [Viewing and Performing Bulk Operations for Internal Identity Store Users, page 8-21](#)
- [Deleting Users from Internal Identity Stores, page 8-17](#)

Configuring Authentication Settings for Hosts

ACS 5.8.1 introduces a new section “Authentication Settings” under “System Administration” for Configuring Authentication Settings for Hosts. Using this section, you can disable and delete host accounts based on their inactivity.

This section describes the following:

- [Disabling and Deleting Host Accounts After N and N+x Days of Inactivity, page 8-22](#)

Disabling and Deleting Host Accounts After *N* and *N+x* Days of Inactivity

Before you Begin:

- This feature is applicable only for the internal hosts that sends MAB authentication requests.
- ACS must be configured to send passed authentication messages to the log collector server.
- The log collector server must be running and receiving syslog messages from all ACS nodes in the deployment.
- The log recovery feature must be enabled.

ACS 5.8.1 allows the administrator to configure the maximum number of days from ACS web interface during which the internal hosts’ accounts are enabled despite the hosts not having logged in to the network. Once the configured period is exceeded, the host’s account is disabled if the host has not logged in to the network. Also, the administrator can configure the number of days in such a way that ACS can delete the host account from the database if the host has not logged in to the network after the host account is disabled.

The default value for disabling the host account is 30 days of inactivity. The default value for deleting the host account is 60 days of inactivity after the host account is disabled. For this feature to work properly, the log collector server should be running and receiving the syslog messages from all ACS nodes in the deployment.

ACS calculates the inactivity based on the last login date of MAB entry. Every day at 10 PM, ACS View runs a job to provide the list of active MAB entries to the primary management. An active host is one which has made at least one successful authentication for the configured period of time. You can observe the last active time of a host from the passed authentication reports in ACS Reports web interface. Based on this list, the primary management identifies the inactive MAB entries list, disables them, and sends an audit log message to the log collector server. The administrator can enable the disabled host account. After enabling the host account, the subsequent calculation for inactivity will be calculated from the last enabled date.

**Note**

When you change the log collector server, it is mandatory to restore the back up taken from the old log collector server in the new log collector server.

**Note**

When you restore the ACS backup from one ACS instance to another ACS instance, the view back up also should be restored along with the ACS backup.

To disable host accounts after n days of inactivity:

Step 1 Choose **System Administration > Hosts > Authentication Settings**.

The Host Authentication Settings page appears.

Step 2 Check the **Disable host account after n days of inactivity** check box.

Step 3 Enter the number of days in the text box.

ACS disables the host account if it is not active for the configured number of days.

To delete host accounts after n days of disablement:

Step 1 Choose **System Administration > Hosts > Authentication Settings**.

The Host Authentication Settings page appears.

Step 2 Check the **Delete host account after n days of disablement/inactivity** check box.

Step 3 Enter the number of days in the text box.

ACS deletes the host account if it is not active for the configured number of days after that account is disabled.

Creating Hosts in Identity Stores

To create, duplicate, or edit a MAC address and assign identity groups to internal hosts:

Step 1 Choose **Users and Identity Stores > Internal Identity Stores > Hosts**.

The Internal Hosts page appears, listing any configured internal hosts.

Step 2 Click **Create**. You can also:

- Check the check box next to the MAC address you want to duplicate, then click **Duplicate**.
- Click the MAC address that you want to modify, or check the check box next to the MAC address and click **Edit**.
- Click **File Operations** to perform bulk operations. See [Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-25](#) for more information on the import process.
- Click **Export** to export a list of hosts to your local hard drive.

The Internal Hosts General page appears when you click the Create, Duplicate, or Edit options.

Step 3 Complete the fields in the Internal MAC Address Properties page as described in [Table 8-6](#):

Table 8-6 Internal Hosts Properties Page

Option	Description
General	
MAC Address	<p>ACS 5.8.1 support wildcards while adding new hosts to the internal identity store. Enter a valid MAC address, using any of the following formats:</p> <ul style="list-style-type: none"> • 01-23-45-67-89-AB/01-23-45-* • 01:23:45:67:89:AB/01:23:45:* • 0123.4567.89AB/0123.45* • 0123456789AB/012345* <p>ACS accepts a MAC address in any of the above formats, and converts and stores the MAC address as six hexadecimal digits separated by hyphens; for example, 01-23-45-67-89-AB.</p>
Status	Use the drop-down list box to enable or disable the MAC address.
Description	(Optional) Enter a description of the MAC address.
Identity Group	Enter an identity group with which to associate the MAC address, or click Select to display the Identity Groups window. Choose an identity group with which to associate the MAC address, then click OK .
MAC Host Information	<i>Display only.</i> Contains MAC host identity attribute information.
Creation/Modification Information	
This section of the page appears only after you have created or modified a MAC address.	
Date Created	<p><i>Display only.</i> The date that the host account was created, in the format <i>Day Mon dd hh:mm:ss UTC YYYY</i>, where:</p> <ul style="list-style-type: none"> • <i>Day</i> = Day of the week. • <i>Mon</i> = Three characters that represent the month of the year: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sept, Oct, Nov, Dec • <i>DD</i> = Two digits that represent the day of the month; a space precedes single-digit days (1 to 9). • <i>hh:mm:ss</i> = Hour, minute, and second, respectively • <i>YYYY</i> = Four digits that represent the year
Date Modified	<p><i>Display only.</i> The date that the host account was last modified (updated), in the format <i>Day Mon dd hh:mm:ss UTC YYYY</i>, where:</p> <ul style="list-style-type: none"> • <i>Day</i> = Day of the week. • <i>Mon</i> = Three characters that represent the month of the year: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sept, Oct, Nov, Dec • <i>DD</i> = Two digits that represent the day of the month; a space precedes single-digit days (1 to 9). • <i>hh:mm:ss</i> = Hour, minute, and second, respectively • <i>YYYY</i> = Four digits that represent the year

Step 4 Click **Submit** to save changes.

The MAC address configuration is saved. The Internal MAC list page appears with the new configuration.

**Note**

Hosts with wildcards (supported formats) for MAC addresses are migrated from 4.x to 5.x.

**Note**

You can add wildcard for MAC address which allows the entire range of Organization Unique Identifier (OUI) clients.

For example: If you add Cisco's MAC address 00-00-0C-*, the entire range of Cisco devices will be added to the host.

Related Topics

- [Host Lookup, page 4-12](#)
- [Deleting Internal Hosts, page 8-25](#)
- [Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-25](#)
- [Policies and Identity Attributes, page 3-17](#)
- [Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17](#)

Deleting Internal Hosts

To delete a MAC address:

-
- Step 1** Choose **Users and Identity Stores > Internal Identity Stores > Hosts**.
- The Internal MAC List page appears, with any configured MAC addresses listed.
- Step 2** Check one or more of the check boxes next to the internal hosts you want to delete.
- Step 3** Click **Delete**.
- The following message appears:
- Are you sure you want to delete the selected item/items?
- Step 4** Click **OK**.
- The Internal MAC List page appears without the deleted MAC addresses.
-

Related Topics

- [Host Lookup, page 4-12](#)
- [Viewing and Performing Bulk Operations for Internal Identity Store Hosts, page 8-25](#)
- [Creating Hosts in Identity Stores, page 8-23](#)
- [Policies and Identity Attributes, page 3-17](#)
- [Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17](#)

Viewing and Performing Bulk Operations for Internal Identity Store Hosts

To view and perform bulk operations for internal identity stores:

Step 1 Choose **Users and Identity Stores > Internal Identity Stores > Hosts**.

The Internal Hosts page appears, with any configured internal hosts listed.

Step 2 Click **File Operations** to perform any of the following functions:

- **Add**—Choose this option to add internal hosts from an import file to ACS.
- **Update**—Choose this option to replace the list of internal hosts in ACS with the internal hosts in the import file.
- **Delete**—Choose this option to delete the internal hosts listed in the import file from ACS.

See [Performing Bulk Operations for Network Resources and Users, page 7-8](#) for a detailed description of the bulk operations.

Related Topics

- [Host Lookup, page 4-12](#)
- [Creating Hosts in Identity Stores, page 8-23](#)
- [Deleting Internal Hosts, page 8-25](#)
- [Policies and Identity Attributes, page 3-17](#)
- [Configuring an Identity Group for Host Lookup Network Access Requests, page 4-17](#)

Management Hierarchy

Management Hierarchy enables the administrator to give access permission to the internal users or internal hosts according to their level of hierarchy in the organizations management hierarchy. A hierarchical label is assigned to each device that represents the administrative location of that particular device within the organizations management hierarchy.

For example, the hierarchical label *All:US:NY:MyMgmtCenter* indicates that the device is in a MyMgmtcenter under NY city which is in U.S. The administrator can give access permission to the users based on their assigned level of hierarchy. For instance, if a user has an assigned level as *All:US:NY*, then that user is given permission when the user accesses the network through any device with a hierarchy that starts with *All:US:NY*. The same examples are applicable for internal hosts.

Attributes of Management Hierarchy

To use the Management Hierarchy feature, administrator needs to create the following attributes in the Internal Users Dictionary:

- **ManagementHierarchy** attribute—allows the administrator to define one or more hierarchies for each internal users or internal hosts. This attribute is of type string and the maximum character length is 256. See [Creating, Duplicating, and Editing an Internal User Identity Attribute, page 18-12](#) and [Creating, Duplicating, and Editing an Internal Host Identity Attribute, page 18-14](#).
- **UserIsInManagementHierarchy** or **HostIsInManagementHierarchy** attribute—the value of this attribute is set to true when the hierarchy defined for the user or host equals or contained in the hierarchy defined for the network device and AAA clients. This attribute is of type Boolean and the default value is false. It is not displayed in the users or hosts page in ACS web interface. You can

view this attribute only in the identity attributes dictionary list. See [Creating, Duplicating, and Editing an Internal User Identity Attribute, page 18-12](#) and [Creating, Duplicating, and Editing an Internal Host Identity Attribute, page 18-14](#).

Configuring AAA Devices for Management Hierarchy

The management centers and the correlated customer names should be configured within a Management Hierarchy for each AAA client. Any Network Device Group can be used as a Management Hierarchy for a AAA client. The Network Device Group used for this is known as the Management Hierarchy Attribute. The administrator can create a new Network Device Group which will be used as Management Hierarchy. The *Location* hierarchy is an example of a Management Hierarchy attribute.

Example:

Location:All Locations:ManagementCenter1:Customer1

Configuring Users or Hosts for Management Hierarchy

A specific level of access is defined to represent the top-most node in the Management Hierarchy assigned for each user or a host. This level is defined in the user's "ManagementHierarchy" attribute. Total value length is limited to 256 characters.

The administrator can configure any level of hierarchy while defining management centers or AAA client locations. The syntax for ManagementHierarchy attribute is:

<HierarchyName>: <HierarchyRoot>:<Value>

Examples:

- *Location:All Locations:ManagementCenter1*
- *Location:All Locations:ManagementCenter1:Customer 1*

The administrator can configure multiple values for management hierarchy. The syntax for multiple value attribute is:

<HierarchyName>: <HierarchyRoot>:<Value>|<Value>|...

Example:

Location:All Locations:ManagementCenter1:Customer1\ManagementCenter1:Customer2

Configuring and Using the UserIsInManagement Hierarchy Attribute

To configure and use the UserIsInManagementHierarchy attribute, complete the following steps:

- Step 1** Create the ManagementHierarchy and UserIsInManagementHierarchy attributes for internal users. See [Configuring Internal Identity Attributes, page 18-13](#).
- Step 2** Create the network device groups for the network devices and AAA clients with the required hierarchies. See [Creating, Duplicating, and Editing Network Device Groups, page 7-2](#).
- Step 3** Create network devices and AAA clients and associate them with a network device group. See [Creating, Duplicating, and Editing Network Devices, page 7-10](#).
- Step 4** Create internal users and configure the ManagementHierarchy attribute. See [Creating Internal Users, page 8-13](#).
- Step 5** Choose **Access Policies > Access Services > Default Network Access > Authorization**.

The Authorization page appears.

Step 6 Click **Customize**, add the compound condition to the policy conditions, and click **OK**.

Step 7 Click **Create** to create a new policy, and do the following:

- a. Enter an appropriate name for the policy, and set the status.
- b. In the Conditions section, check the **Compound Condition** check box.
- c. Select **Internal users** from the dictionary drop-down list.
- d. Select the **UserIsInManagementHierarchy** attribute from the available attribute list.
- e. Select **Static value** and enter **True** as a condition for the rule to be matched.
- f. Click **Add** to add this compound condition to the policy.
- g. Choose the policy result for the rule and click **OK**.

See [Configuring a Session Authorization Policy for Network Access, page 10-31](#), for more information on creating an authorization policy for network access.

Step 8 After successfully creating the policy, try authenticating the user using the created policy. The user will be authenticated only if the hierarchy defined for the user equals or is contained in the AAA clients hierarchy. You can view the logs to analyze the authentication results.

Related Topics

[Configuring and Using the HostIsInManagement Hierarchy Attribute, page 8-28.](#)

Configuring and Using the HostIsInManagement Hierarchy Attribute

To configure and use the HostIsInManagementHierarchy attribute, complete the following steps:

-
- Step 1** Create the ManagementHierarchy and HostIsInManagementHierarchy attributes for internal hosts. See [Configuring Internal Identity Attributes, page 18-13](#).
- Step 2** Create the network device groups for the network devices and AAA clients with the required hierarchies. See [Creating, Duplicating, and Editing Network Device Groups, page 7-2](#).
- Step 3** Create network devices and AAA clients and associate them with a network device group. See [Creating, Duplicating, and Editing Network Devices, page 7-10](#).
- Step 4** Create internal hosts and configure the ManagementHierarchy attribute. See [Creating Internal Users, page 8-13](#).
- Step 5** Choose **Access Policies > Access Services > Default Network Access > Authorization**.
The Authorization page appears.
- Step 6** Click **Customize**, add the compound condition to the policy conditions, and click **OK**.
- Step 7** Click **Create** to create a new policy, and do the following:
- a. Enter an appropriate name for the policy, and set the status.
 - b. In the Conditions section, check the **Compound Condition** check box.
 - c. Select **Internal hosts** from the dictionary drop-down list.
 - d. Select **HostIsInManagementHierarchy** attribute from the available attribute list.
 - e. Select **Static value** and enter **True** as a condition for the rule to be matched.

- f. Click **Add** to add this compound condition to the policy.
- g. Choose the policy result for the rule and click **OK**.

See [Configuring a Session Authorization Policy for Network Access, page 10-31](#), for more information on creating an authorization policy for network access.

Step 8 After successfully creating the policy, try authenticating the user using the created policy. The user will be authenticated only if the hierarchy defined for the user equals or is contained in the AAA clients hierarchy. You can view the logs to analyze the authentication results.

Related Topics

- [Configuring and Using the UserIsInManagement Hierarchy Attribute, page 8-27](#).

Managing External Identity Stores

ACS 5.8.1 integrates with external identity systems in a number of ways. You can leverage an external authentication service or use an external system to obtain the necessary attributes to authenticate a principal, as well to integrate the attributes into an ACS policy.

For example, ACS can leverage Microsoft AD to authenticate a principal, or it could leverage an LDAP bind operation to find a principal in the database and authenticate it. ACS can obtain identity attributes such as AD group affiliation to make an ACS policy decision.



Note

ACS 5.8.1 does not have a built-in check for the dial-in permission attribute for Windows users. You must set the msNPAllowDialin attribute through LDAP or Windows AD. For information on how to set this attribute, refer to Microsoft documentation at:
<http://msdn.microsoft.com/en-us/library/ms678093%28VS.85%29.aspx>

This section provides an overview of the external identity stores that ACS 5.8.1 supports and then describes how you can configure them.

This section contains the following topics:

- [LDAP Overview, page 8-29](#)
- [Leveraging Cisco NAC Profiler as an External MAB Database, page 8-45](#)
- [Microsoft AD, page 8-52](#)
- [RSA SecurID Server, page 8-80](#)
- [RADIUS Identity Stores, page 8-86](#)

LDAP Overview

Lightweight Directory Access Protocol (LDAP), is a networking protocol for querying and modifying directory services that run on TCP/IP and UDP. LDAP is a lightweight mechanism for accessing an x.500-based directory server. RFC 2251 defines LDAP.

ACS 5.8.1 integrates with an LDAP external database, which is also called an identity store, by using the LDAP protocol. See [Creating External LDAP Identity Stores, page 8-34](#) for information about configuring an LDAP identity store.

This section contains the following topics:

- [Directory Service, page 8-30](#)
- [Authentication Using LDAP, page 8-30](#)
- [Multiple LDAP Instances, page 8-31](#)
- [Failover, page 8-31](#)
- [LDAP Connection Management, page 8-31](#)
- [Authenticating a User Using a Bind Connection, page 8-32](#)
- [Group Membership Information Retrieval, page 8-32](#)
- [Attributes Retrieval, page 8-33](#)
- [Certificate Retrieval, page 8-33](#)
- [Creating External LDAP Identity Stores, page 8-34](#)
- [Configuring LDAP Groups, page 8-43](#)
- [Viewing LDAP Attributes, page 8-43](#)

Directory Service

The directory service is a software application, or a set of applications, for storing and organizing information about a computer network's users and network resources. You can use the directory service to manage user access to these resources.

The LDAP directory service is based on a client-server model. A client starts an LDAP session by connecting to an LDAP server, and sends 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 the directory, which is the database that holds the 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 that 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) constructed from attributes in the entry, followed by the parent entry's DN. You can think of the DN as a full filename, and the RDN as a relative filename in a folder.

Authentication Using LDAP

ACS 5.8.1 can authenticate a principal against an LDAP identity store by performing a bind operation on the directory server to find and authenticate the principal. If authentication succeeds, ACS can retrieve groups and attributes that belong to the principal. The attributes to retrieve can be configured in the ACS web interface (LDAP pages). These groups and attributes can be used by ACS to authorize the principal.

To authenticate a user or query the LDAP identity store, ACS connects to the LDAP server and maintains a connection pool. See [LDAP Connection Management, page 8-31](#).

Multiple LDAP Instances

You can create more than one LDAP instance in ACS 5.8.1. By creating more than one LDAP instance with different IP address or port settings, you can configure ACS to authenticate by 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 ACS LDAP identity store instance.

ACS 5.8.1 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 subtree and group directory subtree combination for which ACS should submit authentication requests.

Failover

ACS 5.8.1 supports failover between a primary LDAP server and secondary LDAP server. In the context of LDAP authentication with ACS, failover applies when an authentication request fails because ACS could not connect to an LDAP server.

For example, as when the server is down or is otherwise unreachable by ACS. To use this feature, you must define primary and secondary LDAP servers, and you must set failover settings.

If you set failover settings and if the first LDAP server that ACS attempts to contact cannot be reached, ACS always attempts to contact the other LDAP server.

The first server ACS attempts to contact might not always be the primary LDAP server. Instead, the first LDAP server that ACS attempts to contact depends on the previous LDAP authentications attempts and on the value that you enter in the Failback Retry Delay box.

LDAP Connection Management

ACS 5.8.1 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 opened connections can be different for each LDAP server (primary or secondary) and is determined according to the maximum number of administration connections configured for each server.

ACS retains a list of open LDAP connections (including the bind information) for each LDAP server that is configured in ACS. 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 to the connection manager.

Authenticating a User Using a Bind Connection

ACS sends a bind request to authenticate the user against an LDAP server. The bind request contains the user's DN and user password in clear text. A user is authenticated when the user's DN and password matches the username and password in the LDAP directory.

- **Authentication Errors**—ACS logs authentication errors in the ACS log files.
- **Initialization Errors**—Use the LDAP server timeout settings to configure the number of seconds that ACS waits 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.
 - Incorrect administrator credentials are configured.
- **Bind Errors**

Possible reasons for an LDAP server to return bind (authentication) errors are:

- Filtering errors—A search using filter criteria fails.
- Parameter errors—Invalid parameters were entered.
- User account is restricted (disabled, locked out, expired, password expired, and so on).

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.

Group Membership Information Retrieval

For user authentication, user lookup, and MAC address lookup, ACS must retrieve the 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 two ways:

- **Groups Refer to Subjects**—The group objects contain an attribute that specifies the subject. Identifiers for subjects can be stored in the group as:
 - Distinguished Names (DNs)
 - Plain usernames

- **Subjects Refer to Groups**—The subject objects contain an attribute that specifies the group they belong to.

LDAP identity stores contain the following parameters for group membership information retrieval:

- **Reference Direction**—Specifies the method to use when determining group membership (either Groups to Subjects or Subjects to Groups).
- **Group Map Attribute**—Indicates which attribute contains the group membership information.
- **Group Name Attribute**—Indicates which attribute contains the group name information.
- **Group Object Class**—Determines that you recognize certain objects as groups.
- **Group Search Subtree**—Indicates the search base for group searches.
- **Member Type Option**—Specifies how members are stored in the group member attribute (either as DNs or plain usernames).

Attributes Retrieval

For user authentication, user lookup, and MAC address lookup, ACS must retrieve the subject attributes from LDAP databases. For each instance of an LDAP identity store, an identity store dictionary is created. These dictionaries support attributes of the following data types:

- String
- Integer 64
- IP Address (This can be either an IP version 4 [IPv4] or IP version 6 [IPv6] address.)
- Unsigned Integer 32
- Boolean

For unsigned integers and IP address attributes, ACS converts the strings that it has retrieved to the corresponding data types. If conversion fails, or if no values are retrieved for the attributes, ACS logs a debug message but does not fail the authentication or the lookup process.

You can optionally configure default values for the attributes that ACS can use when the conversion fails or when ACS does not retrieve any values for the attributes.

Certificate Retrieval

If you have configured certificate retrieval as part of user lookup, then ACS must retrieve the value of the certificate attribute from LDAP. To do this, you must have configured certificate attribute in the List of attributes to fetch while configuring an LDAP identity store.

LDAP Server Identity Check

Background

This feature prevents spoofing attacks when Cisco ACS performs user authentication or authorization against an LDAP server (in IPv4).

An LDAP server can be spoofed if an attacker establishes a rogue LDAP server using a real LDAP server IP address (which can be achieved by another attack on the network), and can get a valid LDAP server certificate issued by the same CA.

ACS is required to perform identify verification on the LDAP server's certificate according to RFC 4513—*Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms*.

Feature Overview

ACS matches the data retrieved from the LDAP server's certificate (usually found in the X.509 SAN section; otherwise it is in the CN section) against the data configured by the ACS administrator about that server. Once this authentication check succeeds, the LDAP connection is established; otherwise the ACS discontinues the connection.

The hostname data in the LDAP server's certificate may be in one of the following formats:

- IP address
- DNS
- DNS using the wildcard character “*”

In the first two cases, the matching is straight forward. If the wildcard character is detected, ACS performs two sanity checks to verify that:

- The reconstructed address is of the correct length.
- The reconstructed address has a “.” immediately after the wildcard character.

Creating External LDAP Identity Stores



Note

Configuring an LDAP identity store for ACS has no effect on the configuration of the LDAP database. ACS recognizes the LDAP database, enabling the database to be authenticated against. To manage your LDAP database, see your LDAP database documentation.

When you create an LDAP identity store, ACS also creates:

- A new dictionary for that store with two attributes, ExternalGroups and IdentityDn.
- A custom condition for group mapping from the ExternalGroup attribute; the condition name has the format LDAP:*ID-store-name* ExternalGroups.

You can edit the predefined condition name, and you can create a custom condition from the IdentityDn attribute in the Custom condition page. See [Creating, Duplicating, and Editing a Custom Session Condition, page 9-5](#).

To create, duplicate, or edit an external LDAP identity store:

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**.

The LDAP Identity Stores page appears.

Step 2 Click **Create**. You can also:

- Check the check box next to the identity store that you want to duplicate, and then click **Duplicate**.
- Click the identity store name that you want to modify, or check the box next to the name and click **Edit**.

If you are creating an identity store, the first page of a wizard appears: General.

If you are duplicating an identity store, the **External Identity Stores > Duplicate: *id-store*** page General tab appears, where *id-store* is the name of the external identity store that you chose.

If you are editing an identity store, the **External Identity Stores > Edit: *id-store*** page General tab appears, where *id-store* is the name of the external identity store that you chose.

- Step 3** Complete the Name and Description fields as required.
- Step 4** Check the Enable Password Change check box to modify the password, to detect the password expiration, and to reset the password.
- Step 5** Click **Next**.
- Step 6** Continue with [Configuring an External LDAP Server Connection, page 8-35](#).

**Note**

A NAC guest server can also be used as an external LDAP server. For the procedure to use a NAC guest server as an external LDAP server:
http://www.cisco.com/c/en/us/td/docs/security/nac/guestserver/configuration_guide/20/nacguestserver/g_guestpol.html

Related Topic

- [Deleting External LDAP Identity Stores, page 8-42](#)

Configuring an External LDAP Server Connection

Use the LDAP page to configure an external LDAP identity store.

- Step 1** Choose **Users and Identity Stores > External Identity Stores > LDAP**, and then click any of the following:
- **Create** and follow the wizard.
 - **Duplicate and then Next**. The Server Connection page appears.
 - **Edit**, and then **Next**. The Server Connection page appears.

Table 8-7 *LDAP: Server Connection Page*

Option	Description
Server Connection	
Enable Secondary Server	Check to enable the secondary LDAP server, which is used as a backup in the event that the primary LDAP server fails. If you check this check box, you must enter configuration parameters for the secondary LDAP server.
Always Access Primary Server First	Click to ensure that the primary LDAP server is accessed first, before the secondary LDAP server is accessed.
Failback to Primary Server After <i>min</i> .Minutes	Click to set the number of minutes that ACS authenticates using the secondary LDAP server if the primary server cannot be reached, where <i>min</i> . is the number of minutes. After this time period, ACS reattempts authentication using the primary LDAP server. (Default is 5.)

Table 8-7 LDAP: Server Connection Page (continued)

Option	Description
Enable Deployment Configuration	<p>Check to enable the deployment configuration tab. The primary and secondary hostname fields in the server connection page become read-only fields when you enable the deployment configuration. You need to configure the primary and secondary LDAP server hostname details in the deployment configuration page; the hostname details of the current ACS will appear in the server connection page after saving it.</p> <p>If you check the Enable Secondary Server check box after configuring the primary LDAP server hostname in the deployment configuration page, the mandatory fields such as port number, server timeout, and maximum admin connections are set to zero. You need to fill in these fields with an appropriate value.</p>
Primary Server	
Hostname	Enter the IP address or DNS name of the machine that is running the primary 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 primary 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 by referring to the administrator of the LDAP server.
Anonymous Access	<p>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 accessible to any unauthenticated client.</p> <p>In the absence of specific policy permitting authentication information to be sent to a server, a client should use an anonymous connection.</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.
Admin DN	<p>Enter the distinguished name of the administrator; that is, the LDAP account which, if bound to, permits searching all required users under the User Directory Subtree and permits searching groups.</p> <p>If the administrator specified does not have permission to see the group name attribute in searches, group mapping fails for users that LDAP authenticates.</p>
Password	Enter the LDAP administrator account password.
Use Secure Authentication	Click to use Secure Sockets Layer (SSL) to encrypt communication between ACS and the primary LDAP server. Verify the Port field contains the port number used for SSL on the LDAP server. If you enable this option, you must select a root CA.
Check Server Identity	Check this check box to allow ACS to perform the server identity check while establishing connection with the LDAP server.
Root CA	Select a trusted root certificate authority from the drop-down list box to enable secure authentication with a certificate.
Server Timeout <sec.> Seconds	Enter the number of seconds that ACS waits for a response from the primary LDAP server before determining that the connection or authentication with that server has failed, where <sec.> is the number of seconds. Valid values are 1 to 300. (Default = 10.)

Table 8-7 LDAP: Server Connection Page (continued)

Option	Description
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 Group Directory Subtree. Valid values are 1 to 99. (Default = 8.)
Test Bind To Server	Click to test and ensure that the primary LDAP server details and credentials can successfully bind. If the test fails, edit your LDAP server details and retest.
Secondary Server	
Hostname	Enter the IP address or DNS name of the machine that is running the secondary 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 secondary 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 by viewing DS Properties on the LDAP machine.
Anonymous Access	Click to verify that searches on the LDAP directory occur anonymously. The server does not distinguish who the client is and will allow the client to access (read and update) any data that is configured to be accessible to any unauthenticated client. In the absence of specific policy permitting authentication information to be sent to a server, a client should use an anonymous connection.
Authenticated Access	Click to ensure that searches on the LDAP directory occur with administrative credentials. If so, enter information for the Admin DN and Password fields.
Admin DN	Enter the domain name of the administrator; that is, the LDAP account which, if bound to, permits searching for all required users under the User Directory Subtree and permits searching groups. If the administrator specified does not have permission to see the group name attribute in searches, group mapping fails for users that LDAP authenticates.
Password	Type the LDAP administrator account password.
Use Secure Authentication	Click to use Secure Sockets Layer (SSL) to encrypt communication between ACS and the secondary LDAP server. Verify the Port field contains the port number used for SSL on the LDAP server. If you enable this option, you must select a root CA.
Check Server Identity	Check this checkbox to allow ACS to perform the server identity check while establishing connection with the LDAP server.
Root CA	Select a trusted root certificate authority from the drop-down list box to enable secure authentication with a certificate.
Server Timeout <sec.> Seconds	Type the number of seconds that ACS waits for a response from the secondary LDAP server before determining that the connection or authentication with that server has failed, where <sec.> is the number of seconds. Valid values are 1 to 300. (Default = 10.)

Table 8-7 LDAP: Server Connection Page (continued)

Option	Description
Max Admin Connections	Type 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 Group Directory Subtree. Valid values are 1 to 99. (Default = 8.)
Test Bind To Server	Click to test and ensure that the secondary LDAP server details and credentials can successfully bind. If the test fails, edit your LDAP server details and retest.

Step 2 Click **Next**.

Step 3 Continue with [Configuring External LDAP Directory Organization, page 8-38](#).

Configuring External LDAP Directory Organization

Use this page to configure an external LDAP identity store.

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**, then click any of the following:

- **Create** and follow the wizard until you reach the Directory Organization page.
- **Duplicate**, then click **Next** until the Directory Organization page appears.
- **Edit**, then click **Next** until the Directory Organization page appears.

Table 8-8 LDAP: Directory Organization Page

Option	Description
Schema	
Subject Object class	Value of the LDAP <i>objectClass</i> attribute that identifies the subject. Often, subject records have several values for the <i>objectClass</i> attribute, some of which are unique to the subject, some of which are shared with other object types. This box should contain a value that is not shared. Valid values are from 1 to 20 characters and must be a valid LDAP object type. This parameter can contain any UTF-8 characters. (Default = Person.)
Group Object class	Enter the group object class that you want to use in searches that identify objects as groups. (Default = GroupOfUniqueNames.)
Subject Name Attribute	Name of the attribute in the subject record that contains the subject name. You can obtain this attribute name from your directory server. This attribute specifies the subject name in the LDAP schema. You use this attribute to construct queries to search for subject objects. For more information, refer to the LDAP database documentation. Valid values are from 1 to 20 characters and must be a valid LDAP attribute. This parameter can contain any UTF-8 characters. Common values are <i>uid</i> and <i>CN</i> . (Default = uid.)

Table 8-8 LDAP: Directory Organization Page (continued)

Option	Description
Group Map Attribute	<p>For user authentication, user lookup, and MAC address lookup, ACS must retrieve group membership information from LDAP databases. LDAP servers represent an association between a subject (a user or a host) and a group in one of the following two ways:</p> <ul style="list-style-type: none"> Groups refer to subjects Subjects refer to groups <p>The Group Map Attribute contains the mapping information.</p> <p>You must enter the attribute that contains the mapping information: an attribute in either the subject or the group, depending on:</p> <ul style="list-style-type: none"> If you select the Subject Objects Contain Reference To Groups radio button, enter a subject attribute. If you select Group Objects Contain Reference To Subjects radio button, enter a group attribute.
Group Name Attribute	<p>Name of the attribute in the group record that contains the group name. You can obtain this attribute name from your directory server. This attribute specifies the group name in the LDAP schema. You use this attribute to construct queries to search for group objects.</p> <p>For more information, refer to the LDAP database documentation. Common values are DN and CN. (Default = DN.).</p>
Certificate Attribute	Enter the attribute that contains certificate definitions. These definitions can optionally be used to validate certificates presented by clients when defined as part of a certificate authentication profile. In such cases, a binary comparison is performed between the client certificate and the certificate retrieved from the LDAP identity store.
Subject Objects Contain Reference To Groups	Click if the subject objects contain a reference to groups.
Group Objects Contain Reference To Subjects	Click if the group objects contain a reference to subjects.
Subjects In Groups Are Stored In Member Attribute As	<p>Use the drop-down list box to indicate if the subjects in groups are stored in member attributes as either:</p> <ul style="list-style-type: none"> Username Distinguished name
Directory Structure	
Subject Search Base	<p>Enter the distinguished name (DN) for the subtree that contains all subjects. For example:</p> <pre>o=corporation.com</pre> <p>If the tree containing subjects is the base DN, enter:</p> <pre>o=corporation.com</pre> <p>or</p> <pre>dc=corporation,dc=com</pre> <p>as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.</p>

Table 8-8 LDAP: Directory Organization Page (continued)

Option	Description
Group Search Base	<p>Enter the distinguished name (DN) for the subtree that contains all groups. For example:</p> <pre>ou=organizational unit[,ou=next organizational unit]o=corporation.com</pre> <p>If the tree containing groups is the base DN, type:</p> <pre>o=corporation.com</pre> <p>or</p> <pre>dc=corporation,dc=com</pre> <p>as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.</p>
Test Configuration	Click to obtain the expected connection and schema results by counting the number of users and groups that may result from your configuration.
Username Prefix\Suffix Stripping	
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, ACS finds the delimiter character that is specified in the <i>start_string</i> box, it strips all characters from the beginning of the username through the delimiter character.</p> <p>If the username contains more than one of the characters that are specified in the <i>start_string</i> box, ACS strips characters through the last occurrence of the delimiter character. For example, if the delimiter character is the backslash (\) and the username is DOMAIN\echamberlain, ACS submits echamberlain to an LDAP server.</p> <p>The <i>start_string</i> cannot contain the following special characters: the pound sign (#), the question mark (?), the quote ("), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). ACS does not allow these characters in usernames. If the X box contains any of these characters, stripping fails.</p>
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, ACS finds the delimiter character that is specified in the Y box, it strips all characters from the delimiter character through the end of the username.</p> <p>If the username contains more than one of the character specified in the Y box, ACS strips characters starting with the first occurrence of the delimiter character. For example, if the delimiter character is the at symbol (@) and the username is <i>jwiedman@domain</i>, then ACS submits <i>jwiedman</i> to an LDAP server.</p> <p>The <i>end_string</i> box cannot contain the following special characters: the pound sign (#), the question mark (?), the quote ("), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). ACS does not allow these characters in usernames. If the <i>end_string</i> box contains any of these characters, stripping fails.</p>

Table 8-8 LDAP: Directory Organization Page (continued)

Option	Description
MAC Address Format	
Search for MAC Address in Format <i><format></i>	<p>MAC addresses in internal identity stores are stored in the format xx-xx-xx-xx-xx-xx. MAC addresses in LDAP databases can be stored in different formats. However, when ACS receives a host lookup request, ACS converts the MAC address from the internal format to the format that is specified in this field.</p> <p>Use the drop-down list box to enable search for MAC addresses in a specific format, where <i><format></i> can be any one of the following:</p> <ul style="list-style-type: none"> • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx • xxxx.xxxx.xxxx <p>The format you select must match the format of the MAC address stored in the LDAP server.</p>

Step 2 Click Next.

Continue with [Configuring LDAP Hostnames in Deployment Configuration, page 8-41](#).

Related Topics

- [Configuring LDAP Groups, page 8-43](#)
- [Deleting External LDAP Identity Stores, page 8-42](#)

Configuring LDAP Hostnames in Deployment Configuration

ACS 5.8.1 supports configuring different LDAP hostnames for different ACS instances in your deployment. Configuring all ACS instances in your deployment to communicate to a single LDAP server may affect the performance of that LDAP server. Also, if your LDAP servers are deployed in different locations, you can configure the ACS instance with the LDAP server that is deployed geographically closer to it. This type of configuration results in better response time. Therefore, to manage the load and increase the performance level, configure in such a way that different ACS instances communicate to different LDAP servers, preferably with the LDAP server deployed in your local geographical location.

ACS introduces a new tab called Deployment Configuration to configure different LDAP server hostnames for every ACS instance. After saving the configuration in Deployment Configuration page, the LDAP server hostnames are auto-populated in the Server Connection page. This configuration can be performed only from the primary ACS instance in a deployment. From the secondary ACS instance, you can only view the details of the LDAP configurations.

If you enable the LDAP Deployment Configurations in your deployment, when a request comes to one of the ACS instances, the ACS instance searches for the configured primary LDAP server. After finding the configured LDAP server, it communicates with that LDAP server and fetches the required details.

Before You Begin

Check the **Enable Deployment Configuration** check box in the Server Connection page. When you check the Enable Deployment Configuration check box, the primary and secondary LDAP server hostname fields become read-only fields.

Use this page to configure different primary and secondary LDAP hostnames for different ACS instances in your deployment:

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP** and then click any of the following:

- **Create** and follow the wizard until you reach the Deployment Configuration page.
- **Duplicate** and then click **Next** until the Deployment Configuration page appears.
- **Edit** and then click **Next** until the Deployment Configuration page appears.



Note

Check the Enable Deployment Configuration check box to enable the Deployment Configuration tab operations. You can see the Deployment Configuration tab even though you have not checked the Deployment Configuration check box. If this Enable Deployment Configuration check box is unchecked, you cannot configure different primary and secondary LDAP server hostnames for the ACS instances in your deployment.

The Deployment Configuration page appears, displaying the current list of ACS instances that are active in your deployment.

Step 2 Check the check box near the ACS instance name and click **Edit**.

The LDAP hostname setting dialog box appears.

This dialog box contains the following two fields:

- **Primary Hostname**—Enter the hostname of the primary LDAP server so that the selected ACS instance communicates with the specified primary LDAP server.
- **Secondary Hostname**—Enter the hostname of the secondary LDAP server so that the selected ACS instance communicates with the specified secondary LDAP server when the primary LDAP server is down.

Step 3 Click **OK**.

The LDAP hostname configuration is saved.

Step 4 Click **Finish**.

The external identity store that you have created is saved.

Related Topics

- [Creating External LDAP Identity Stores, page 8-34](#)
- [Deleting External LDAP Identity Stores, page 8-42](#)

Deleting External LDAP Identity Stores

You can delete one or more external LDAP identity stores simultaneously.

To delete an external LDAP identity store:

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**.

The LDAP Identity Stores page appears, with a list of your configured external identity stores.

Step 2 Check one or more check boxes next to the external identity stores you want to delete.

Step 3 Click **Delete**.

The following error message appears:

Are you sure you want to delete the selected item/items?

Step 4 Click **OK**.

The External Identity Stores page appears, without the deleted identity stores in the list.

Related Topic

- [Creating External LDAP Identity Stores, page 8-34](#)

Configuring LDAP Groups

Use this page to configure an external LDAP group.

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**, then click any of the following:

- **Create** and follow the wizard.
- **Duplicate**, then click the **Directory Groups** tab.
- **Edit**, then click the **Directory Groups** tab.

The Selected Directory Groups field displays a list of groups that are available as options in rule-table group-mapping conditions.

Step 2 Do one of the following:

- Click **Select** to open the Groups secondary window from which you can select groups and add them to the Selected Directory Groups list.
- You can alternatively enter the LDAP groups in the Group Name field and click **Add**.

To remove a selected group from the Selected Directory Groups list, select that group in the Selected Directory Groups list and Click **Deselect**.

Step 3 Click **Submit** to save your changes.

Viewing LDAP Attributes

Use this page to view the external LDAP attributes.

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**.

Step 2 Check the check box next to the LDAP identity store whose attributes you want to view, click **Edit**, and then click the **Directory Attributes** tab.

Step 3 In the Name of example Subject to Select Attributes field, enter the name of an example object from which to retrieve attributes, then click **Select**.

For example, the object can be an user and the name of the object could either be the username or the user's DN.

Step 4 Complete the fields as described in [Table 8-9](#).

Table 8-9 LDAP: Attributes Page

Option	Description
Attribute Name	Type an attribute name that you want included in the list of available attributes for policy conditions.
Type	Select the type you want associated with the attribute name you entered in the Attribute Name field.
Default	<p>Specify the default value you want associated with the attribute name you entered in the Attribute Name field. If you do not specify a default value, no default is used.</p> <p>When attributes are imported to the Attribute Name/Type/Default box via the Select button, these default values are used:</p> <ul style="list-style-type: none"> String—Name of the attribute Integer 64 IP Address—This can be either an IP version 4 (IPv4) or IP version 6 (IPv6) address. Unsigned Integer 32 Boolean
Policy Condition Name	(Optional) Specify the name of the custom condition for this attribute. This condition will be available for selection when customizing conditions in a policy.

Step 5 Click **Add** and the information you entered is added to the fields on the screen.

The attributes listed here are available for policy conditions.

Step 6 Click **Submit** to save your changes.

Configuring LDAP Deployments

Use this page to view the external LDAP attributes.

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**.

Step 2 Check the check box next to the LDAP identity store whose attributes you want to view, click **Edit**, and then click the **Directory Attributes** tab.

Step 3 In the Name of example Subject to Select Attributes field, enter the name of an example object from which to retrieve attributes, then click **Select**.

For example, the object can be an user and the name of the object could either be the username or the user's DN.

Step 4 Complete the fields as described in [Table 8-9](#).

Table 8-10 LDAP: Attributes Page

Option	Description
Attribute Name	Type an attribute name that you want included in the list of available attributes for policy conditions.
Type	Select the type you want associated with the attribute name you entered in the Attribute Name field.

Table 8-10 LDAP: Attributes Page (continued)

Option	Description
Default	<p>Specify the default value you want associated with the attribute name you entered in the Attribute Name field. If you do not specify a default value, no default is used.</p> <p>When attributes are imported to the Attribute Name/Type/Default box via the Select button, these default values are used:</p> <ul style="list-style-type: none"> • String—Name of the attribute • Integer 64 • IP Address—This can be either an IP version 4 (IPv4) or IP version 6 (IPv6) address. • Unsigned Integer 32 • Boolean
Policy Condition Name	(Optional) Specify the name of the custom condition for this attribute. This condition will be available for selection when customizing conditions in a policy.

Step 5 Click **Add** and the information you entered is added to the fields on the screen.

The attributes listed here are available for policy conditions.

Step 6 Click **Submit** to save your changes.

Leveraging Cisco NAC Profiler as an External MAB Database

ACS communicates with Cisco NAC Profiler to enable non-802.1X-capable devices to authenticate in 802.1X-enabled networks. Endpoints that are unable to authenticate through 802.1X use the MAC Authentication Bypass (MAB) feature in switches to connect to an 802.1X-enabled network.

Typically, non-user-attached devices such as printers, fax machines, IP phones, and Uninterruptible Power Supplies (UPSs) are not equipped with an 802.1x supplicant.

This means the switch port to which these devices attach cannot authenticate them using the 802.1X exchange of device or user credentials and must revert to an authentication mechanism other than port-based authentication (typically endpoint MAC address-based) in order for them to connect to the network.

Cisco NAC Profiler provides a solution for identifying and locating the endpoints that are unable to interact with the authentication component of these systems so that these endpoints can be provided an alternative mechanism for admission to the network.

NAC Profiler consists of an LDAP-enabled directory, which can be used for MAC Authentication Bypass (MAB). Thus, the NAC Profiler acts as an external LDAP database for ACS to authenticate non-802.1X-capable devices.



Note

You can use the ACS internal host database to define the MAC addresses for non-802.1X-capable devices. However, if you already have a NAC Profiler in your network, you can use it to act as an external MAB database.

To leverage Cisco NAC Profiler as an external MAB database, you must:

- Enable the LDAP Interface on Cisco NAC Profiler. See [Enabling the LDAP Interface on Cisco NAC Profiler to Communicate with ACS](#), page 8-46.
- Configure NAC Profiler in ACS. See [Configuring NAC Profile LDAP Definition in ACS for Use in Identity Policy](#), page 8-48.

Enabling the LDAP Interface on Cisco NAC Profiler to Communicate with ACS



Note

Before you can enable the LDAP interface on the NAC Profiler, ensure that you have set up your NAC Profiler with the NAC Profiler Collector. For more information on configuring Cisco NAC Profiler, refer to the *Cisco NAC Profiler Installation and Configuration Guide*, available under <http://www.cisco.com/c/en/us/support/security/nac-profiler/products-installation-and-configuration-guides-list.html>.

To enable the LDAP interface on the NAC Profiler to communicate with ACS:

- Step 1** Log into your Cisco NAC Profiler.
- Step 2** Choose **Configuration > NAC Profiler Modules > List NAC Profiler Modules**.
- Step 3** Click **Server**.
The Configure Server page appears.
- Step 4** In the LDAP Configuration area, check the **Enable LDAP** check box as shown in [Figure 8-1](#).

Figure 8-1 LDAP Interface Configuration in NAC Profiler

Configure Server

Server Name: Server

Database Maintenance

Endpoint Timeout: 0 days

Historical limit: 30 days

Network Mapping Configuration

Mapping interval [layer 2]: 60 minutes

Mapping interval [layer 3]: 30 minutes

Distribute load over: 15 minutes

Active Profiling Configuration

Frequency: 60 minutes

Profiling Configuration

Aging Interval: 0 days

Age Penalty: 0 %

LDAP Configuration:

Enable LDAP: ☒

Verbose logging: ☒

276678

- Step 5** Click **Update Server**.
- Step 6** Click the **Configuration** tab and click **Apply Changes**.

The Update NAC Profiler Modules page appears.

- Step 7** Click **Update Modules** to enable LDAP to be used by ACS.

You must enable the endpoint profiles that you want to authenticate against the Cisco NAC Profiler. For information on how to do this, see [Configuring Endpoint Profiles in NAC Profiler for LDAP Authentication](#), page 8-47.

For proper Active Response Events you need to configure Active Response Delay time from your Cisco NAC Profiler UI. For this, choose **Configuration > NAC Profiler Modules > Configure Server > Advanced Options > Active Response Delay**.

Configuring Endpoint Profiles in NAC Profiler for LDAP Authentication

For the non-802.1X endpoints that you want to successfully authenticate, you must enable the corresponding endpoint profiles in NAC Profiler for LDAP authentication.



Note

If the profile is not enabled for LDAP, the endpoints in the profile will not be authenticated by the Cisco NAC Profiler.

To enable the endpoint profiles for LDAP authentication:

-
- Step 1** Log into your NAC Profiler.
- Step 2** Choose **Configuration > Endpoint Profiles > View/Edit Profiles List**.
A list of profiles in a table appears.
- Step 3** Click the name of a profile to edit it.
- Step 4** On the Save Profile page, ensure that the LDAP option is enabled by clicking the **Yes** radio button, if it is not already done as shown in [Figure 8-2](#).

Figure 8-2 *Configuring Endpoint Profiles in NAC Profiler*

Step 5 Click **Save Profile**.

Configuring NAC Profile LDAP Definition in ACS for Use in Identity Policy

After you install ACS, there is a predefined LDAP database definition for NAC Profiler. This predefined database definition for NAC Profiler contains all the required data for establishing an initial connection. The only exception is the host information, which depends on your specific deployment configuration.

The steps below describe how to configure the host information, verify the connection, and use the profile database in policies.



Note

Make sure that ACS NAC Profiler is chosen under **Access Policies > Access Services > Default Network Access > Identity**.



Note

The **NAC Profiler** template in ACS, available under the LDAP external identity store, works with Cisco NAC Profiler version 2.1.8 and later.

To edit the NAC Profiler template in ACS:

Step 1 Choose **Users and Identity Stores > External Identity Stores > LDAP**.

Step 2 Click on the name of the NAC Profiler template or check the check box next to the NAC Profiler template and click **Edit**.

The Edit NAC Profiler definition page appears as shown in [Figure 8-3](#).

Figure 8-3 *Edit NAC Profiler Definition — General Page*

Users and Identity Stores > External Identity Stores > LDAP > Edit: *NAC Profiler*

General | Server Connection | Directory Organization | Directory Groups | Directory Attributes

Name: NAC Profiler

Description: Default Entry for NAC Profiler

Database Type: LDAP

* = Required fields

- Step 3** Click the **Server Connection** tab.
- The Edit page appears as shown in [Figure 8-4](#).

Figure 8-4 *Edit NAC Profiler Definition — Server Connection Page*

General | **Server Connection** | Directory Organization | Directory Groups | Directory Attributes

Server Connection

☐ Enable Secondary Server ☐ Always Access Primary Server First

☒ Failback To Primary Server After: 5 Minutes

Primary Server

Hostname: your.hostname.here

Port: 389

☐ Anonymous Access ☒ Authenticated Access

Admin DN: cn=root,o=beacon

Password: *

☐ Use Secure Authentication

Root CA: *

Server Timeout: 10 Seconds

Max. Admin Connections: 20

Test Bind To Server

Secondary Server

Hostname: *

Port: *

☐ Anonymous Access ☐ Authenticated Access

Admin DN: *

Password: *

☐ Use Secure Authentication

Root CA: *

Server Timeout: 0 Seconds

Max. Admin Connections: 0

Test Bind To Server

* = Required fields

- Step 4** In the **Primary Server Hostname** field, enter the IP address or fully qualified domain name of the Profiler Server, or the Service IP of the Profiler pair if Profiler is configured for High Availability.
- Step 5** Click **Test Bind to Server** to test the connection and verify ACS can communicate with Profiler through LDAP.

A small popup dialog, similar to the one shown in [Figure 8-5](#) appears.

Figure 8-5 Test Bind to Server Dialog Box

For more information, see [Creating External LDAP Identity Stores](#), page 8-34.

**Note**

The default password for LDAP is *GBSbeacon*. If you want to change this password, refer to the [Cisco NAC Profiler Installation and Configuration Guide](#).

- Step 6** If successful, go to the **Directory Organization** tab.
The Edit page appears as shown in [Figure 8-6](#).

Figure 8-6 Edit NAC Profiler Definition — Directory Organization Page

 A screenshot of the 'Edit NAC Profiler Definition' page in the Cisco NAC Profiler interface. The page has several tabs: 'General', 'Server Connection', 'Directory Organization' (which is selected), 'Directory Groups', and 'Directory Attributes'. Under the 'Directory Organization' tab, there are sections for 'Schema', 'Directory Structure', 'Username Prefix/Suffix Stripping', and 'MAC Address Format'. The 'Schema' section includes fields for 'Subject Objectclass', 'Subject Name Attribute', 'Group Objectclass', 'Group Map Attribute', 'Group Name Attribute', and 'Certificate Attribute'. The 'Directory Structure' section has 'Subject Search Base' and 'Group Search Base' fields. The 'Username Prefix/Suffix Stripping' section has checkboxes for stripping subject names. The 'MAC Address Format' section has a dropdown for 'Search for MAC Address in Format'. A 'Test Configuration' button is located below the 'Directory Structure' section. A legend at the bottom left indicates that orange asterisks denote required fields.

- Step 7** Click **Test Configuration**.

A dialog box as shown in [Figure 8-7 on page 50](#) appears that lists data corresponding to the Profiler. For example:

- Primary Server
- Number of Subjects: 100
- Number of Directory Groups: 6

Figure 8-7 Test Configuration Dialog Box



Number of Subjects—This value maps to the actual subject devices already profiled by the Cisco NAC Profiler (actual devices enabled for Profiler).

After the Profiler receives initial SNMP trap information from the switch, Profiler can poll the switch using SNMP to gather MIB (Management Information Base) information about the switch as well as the connecting endpoint.

After the Profiler has learned about the endpoint (e.g. MAC address, switch port), it adds the endpoint to its database. An endpoint added to the Profiler's database is considered 1 subject.

Number of Directory Groups—This value maps to the actual profiles enabled for LDAP on Profiler. When already running Profiler on your network, default profiles for endpoints are pre-configured.

However, all profiles are not enabled for LDAP, and must be configured as described in [Configuring Endpoint Profiles in NAC Profiler for LDAP Authentication, page 8-47](#). Note that if setting up Profiler for the first time, once the Profiler is up and running, you will see zero groups initially.

The subjects and directory groups are listed if they are less than 100 in number. If the number of subjects or directory groups exceed 100, the subjects and directory groups are not listed. Instead, you get a message similar to the following one:

More than 100 subjects are found.

Step 8 Click the Directory Attributes tab if you want to use the directory attributes of subject records as policy conditions in policy rules. See [Viewing LDAP Attributes, page 8-43](#) for more information.

Step 9 Choose NAC Profiler as the result (Identity Source) of the identity policy. For more information, see [Viewing Identity Policies, page 10-23](#).

As soon as Endpoint is successfully authenticated from ACS server, ACS will do a CoA (Change of Authorization) and change VLAN. For this, you can configure static VLAN mapping in ACS server. For more information, see [Specifying Common Attributes in Authorization Profiles, page 9-19](#).

When Endpoint is successfully authenticated the following message is displayed on the switch.

```
ACCESS-Switch# #show authentication sessions
Interface MAC Address Method Domain Status Session ID
Fa1/0/1 0014.d11b.aa36 mab DATA Authz Success 505050010000004A0B41FD15
```

For more information on features like Event Delivery Method and Active Response, see the [Cisco NAC Profiler Installation and Configuration Guide, Release 3.1](#).



Note

You can use Microsoft Active Directory as an LDAP server and authenticate against ACS.

Troubleshooting MAB Authentication with Profiler Integration

To troubleshoot MAB authentication while integrating with NAC Profiler and to verify that the endpoint is successfully authenticated, complete the following steps:

Step 1 Run the following command on the switch which is connected to the endpoint devices:

```
ACCESS-Switch# show authentication sessions
```

The following output is displayed:

Interface	MAC Address	Method	Domain	Status	Session ID
Fa1/0/1	0014.d11b.aa36	mab	DATA	Authz Success	505050010000004A0B41FD15 reject

Step 2 Enable debugging for SNMP, AAA, and 802.1X on the switch.

Step 3 Verify the MAB authentication logs in **Monitoring and Reports Viewer > Troubleshooting**, for failure and success authentications.

Microsoft AD

ACS uses Microsoft Active Directory (AD) as an external identity store to store resources such as, users, machines, groups, and attributes. ACS authenticates these resources against AD.

Supported Authentication Protocols

- EAP-FAST and PEAP—ACS supports user and machine authentication and change password against AD using EAP-FAST and PEAP with an inner method of MSCHAPv2 and EAP-GTC.
- PAP—ACS supports authenticating against AD using TACACS PAP or ASCII method and also allows you to change AD users password.
- MSCHAPv1—ACS supports user and machine authentication against AD using MSCHAPv1. You can change AD users password using MSCHAPv1 version 2. ACS does not support MS-CHAP MPPE-Keys of a user, but does support MPPE-Send-Key and MPPE-Recv-Key.



Note

ACS does not support changing user password against AD using MSCHAP version 1.

- MSCHAPv2—ACS supports user and machine authentication against AD using MSCHAPv2. ACS does not support MS-CHAP MPPE-Keys of a user, but does support MPPE-Send-Key and MPPE-Recv-Key.
- EAP-GTC—ACS supports user and machine authentication against AD using EAP-GTC.
- EAP-TLS—ACS uses the certificate retrieval option to support user and machine authentication against AD using EAP-TLS.

ACS 5.x supports changing the password for users who are authenticated against Active Directory in the TACACS+ PAP/ASCII, EAP-MSCHAP, and EAP-GTC methods. Changing the password for EAP-FAST and PEAP with inner MSCHAPv2 is also supported.

Changing the AD user password using the above methods must comply with the AD password policies. You must check with your AD administrator to determine the complete set of AD password policy rules. The most important AD password policies are:

- Enforce password history: N passwords are remembered.

- Maximum password age is N days.
- Minimum password age is N days.
- Minimum password length is N characters.
- Password must meet complexity requirements.

AD uses the “Maximum password age is N days” rule to detect password expiry. All other rules are used during attempts to change a password.

ACS supports these AD domains:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2012 R2 update 2

ACS machine access restriction (MAR) features use AD to map machine authentication to user authentication and authorization, and sets a the maximal time allowed between machine authentication and an authentication of a user from the same machine.

Most commonly, MAR fails authentication of users whose host machine does not successfully authenticate or if the time between machine and user authentication is greater than the specified aging time. You can add MAR as a condition in authentication and authorization rules as required.

While trying to join ACS to the AD domain, ACS and AD must be time-synchronized. Time in ACS is set according to the Network Time Protocol (NTP) server. Both AD and ACS should be synchronized by the same NTP server. If time is not synchronized when you join ACS to the AD domain, ACS displays a clock skew error. Using the command line interface on your appliance, you must configure the NTP client to work with the same NTP server that the AD domain is synchronized with.

The NTP process restarts automatically when it is down. You can check the NTP process status in two ways:

- Use the `sh app status acs` command in CLI interface.
- Choose **Monitoring and Reports > Reports > ACS Reports > ACS Instance > ACS_Health_Summary** in the ACS web interface.

For more information, see [CLI Reference Guide for Cisco Secure Access Control System 5.8.1](#).

**Note**

ACS supports two way trust between Active Directory domains.

The ACS appliance uses different levels of caching for AD groups, to optimize performance. AD groups are identified with a unique identifier, the Security Identifier (SID). ACS retrieves the SID that belongs to the user, and uses the cached mapping of the SID with the full name and path of the group. The AD client component caches the mapping for 24 hours. The run-time component of ACS queries the AD client and caches the results, as long as ACS is running.

**Note**

To prevent ACS from using the outdated mappings, you should create new AD groups instead of changing or moving the existing ones. If you change or move the existing groups, you have to wait for 24 hours and restart the ACS services to refresh all the cached data.

Related Topics

- [Prerequisites for Integrating Active Directory and ACS, page 8-54](#)
- [Network Ports That Must Be Open for Active Directory Communication, page 8-55](#)

Prerequisites for Integrating Active Directory and ACS

The following are the prerequisites to integrate Active Directory with ACS.

- Use the Network Time Protocol (NTP) server settings to synchronize the time between the ACS server and Active Directory. You can configure NTP settings from ACS CLI.
- If your Active Directory structure has multi-domain forest or is divided into multiple forests, ensure that trust relationships exist between the domains to which ACS 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 ACS, in the domain to which you are joining ACS.

Table 8-11 *Active Directory Account Permissions Required for Performing Various Operations*

Join Operations	Leave Operations	ACS 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 ACS machine account already exists) • Create ACS machine account to domain (if the machine account does not already exist) • Set attributes on the new machine account (for example, ACS machine account password, SPN, dnsHostname) <p>Note 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 ACS machine account already exists) • Remove ACS machine account from domain <p>Note If you perform a force leave (leave without domain credentials), it will not remove the machine account from the domain.</p>	<p>For the newly created ACS 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 or machine objects corresponding to users or 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>Note You can precreate the machine account in Active Directory, and if the SAM name matches the ACS appliance hostname, it should be located during the join operation and re-used.</p> <p>Note If multiple join operations are performed, multiple machine accounts are maintained inside ACS, one for each join operation.</p>

**Note**

The credentials used for the join or leave operation are not stored in ACS. Only the newly created ACS machine account credentials are stored.

Related Topics

[Network Ports That Must Be Open for Active Directory Communication, page 8-55](#)

Network Ports That Must Be Open for Active Directory Communication

ACS supports certificate authorization. If there is a firewall between ACS and AD, certain ports need to be opened in order to allow ACS to communicate with AD. The following are the default ports to be opened:

Table 8-12 *Network Ports That Must Be Open for Active Directory Communication*

Protocol	Port (remote-local)	Target	Authenticated	Comments
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	—
KPASS	464	Domain Controllers	Yes (Kerberos)	MS AD/KDC
DNS (TCP/UDP)	53	DNS Servers/AD Domain Controllers	No	—
IPC	80	Other ACS nodes in the Deployment	Yes (Using RBAC credentials)	—

**Note**

Dial-in users are not supported by AD in ACS.

This section contains the following topics:

- [Machine Authentication, page 8-56](#)
- [Attribute Retrieval for Authorization, page 8-56](#)
- [Group Retrieval for Authorization, page 8-61](#)
- [Certificate Retrieval for EAP-TLS Authentication, page 8-61](#)
- [Concurrent Connection Management, page 8-62](#)
- [User and Machine Account Restrictions, page 8-62](#)
- [Machine Access Restrictions, page 8-62](#)
- [Dial-In Permissions, page 8-65](#)
- [Callback Options for Dial-In users, page 8-66](#)
- [Joining ACS to an AD Domain, page 8-67](#)
- [Selecting an AD Group, page 8-73](#)
- [Configuring AD Attributes, page 8-74](#)

- [Configuring Machine Access Restrictions, page 8-76](#)
- [Advanced Tuning, page 8-77](#)
- [Configuring Authentication Domains, page 8-77](#)
- [Diagnose Active Directory Problems, page 8-78](#)
- [Active Directory Alarms and Reports, page 8-79](#)

Machine Authentication

Machine authentication provides access to network services to only those computers that are listed in Active Directory. This becomes very important for wireless networks because unauthorized users can try to access your wireless access points from outside your office building.

Machine authentication happens while starting up a computer or while logging in to a computer. Supplicants, such as Funk Odyssey perform machine authentication periodically while the supplicant is running.

If you enable machine authentication, ACS authenticates the computer before a user authentication request comes in. ACS checks the credentials provided by the computer against the Windows user database. If the credentials match, the computer is given access to the network.



Note

When you perform Machine Authentication using EAP-TLS protocol, you should enable the “Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory” option and select the appropriate LDAP or Active Directory in the **Certificate Authentication Profile > CN User Name > Edit Page**.

Related Topics

- [Attribute Retrieval for Authorization, page 8-56](#)
- [Boolean Attribute Support in Active Directory or LDAP, page 8-57](#)
- [Multi-Value Attribute Support in AD or LDAP, page 8-58](#)
- [Group Retrieval for Authorization, page 8-61](#)
- [Certificate Retrieval for EAP-TLS Authentication, page 8-61](#)

Attribute Retrieval for Authorization

You can configure ACS to retrieve Active Directory user or machine attributes to be used in authorization and group-mapping rules. The attributes are mapped to the ACS policy results and determine the authorization level for the user or machine.

ACS retrieves the user and Active Directory machine attributes after a successful user or machine authentication; ACS can also retrieve the attributes for authorization and group-mapping purposes independent of authentication.

msRADIUSFramedIPAddress Attribute

In ACS, you can configure the Framed-IP-Address attribute as a dynamic value so that it takes the value dynamically from the AD attribute, msRADIUSFramedIPAddress during authentication. You can use the msRADIUSFramedIPAddress attribute that is retrieved from AD only as the IP address in ACS. You cannot convert this attribute type to string, integer, Boolean, and so on.

In AD, for every dial-in user, the AD administrator assigns a static IP address. When a dial-in user tries to connect to a network, the request is routed to ACS. ACS processes that request, authenticates the user against AD, and assigns the static IP address that is retrieved from AD to the dial-up client that is trying to connect to the network. In ACS 5.8.1, the msRADIUSFramedIPAddress attribute is of type IP Address.

You must configure the msRADIUSFramedIPAddress attribute in the Directory Attributes tab of Active Directory configuration in ACS and also use this attribute in the network access authorization profile for ACS to assign this value to the dial-up client. For more information on the network access authorization profile, see [Authorization Profiles for Network Access, page 3-16](#).

Related Topics

- [Boolean Attribute Support in Active Directory or LDAP, page 8-57](#)
- [Multi-Value Attribute Support in AD or LDAP, page 8-58](#)
- [Group Retrieval for Authorization, page 8-61](#)
- [Certificate Retrieval for EAP-TLS Authentication, page 8-61](#)

Boolean Attribute Support in Active Directory or LDAP

ACS 5.8.1 allows you to configure Boolean attributes in AD or the LDAP Directory Attributes page and retrieves Boolean attributes from AD or LDAP during authentication against an AD or LDAP identity store. ACS retrieves the attributes specific to a user who is trying to authenticate against an AD or LDAP identity store.

ACS supports the following values for Boolean attributes:

- True—t, T, true, TRUE, True, and 1.
- False—f, F, false, FALSE, False, and 0.

You can configure Boolean attributes in AD or the LDAP Directory Attributes page and use them in authorization profiles. ACS does not recognize the Boolean attribute if you configure a value other than the supported values listed above.

- You can configure the Boolean attribute of AD or LDAP as a string. ACS converts the Boolean value of the specific attribute to a string value while retrieving it from AD or LDAP.

For example, consider the Boolean attribute msTSAllowLogon.

In AD or LDAP, the attribute msTSAllowLogon is a Boolean attribute. In ACS, you can configure the msTSAllowLogon attribute as string.

- If the value of a Boolean attribute in AD or LDAP is 0 or 1, you can convert that attribute to an integer.
- The Boolean attribute in AD or LDAP can be retrieved only as an attribute of type Boolean in ACS.
- You can also configure a string or an integer type AD or LDAP attribute as a Boolean attribute in ACS.

For example, consider the attribute displayName.

In AD or LDAP, the attribute displayName is a string or integer type attribute. In ACS, you can configure displayName as Boolean only when the value for the displayName attribute is one of the supported Boolean values listed above.



Note

ACS does not support attribute substitution for Boolean attributes in RADIUS and TACACS+ authentications.

Related Topics

- [Attribute Retrieval for Authorization, page 8-56](#)
- [Multi-Value Attribute Support in AD or LDAP, page 8-58](#)
- [Group Retrieval for Authorization, page 8-61](#)
- [Certificate Retrieval for EAP-TLS Authentication, page 8-61](#)

Multi-Value Attribute Support in AD or LDAP

ACS 5.8.1 allows you to configure multi-value attributes in AD or the LDAP Directory Attributes page and retrieves multi-value attributes from AD or LDAP during authentication against an AD or LDAP identity store. ACS retrieves the attributes specific to a user who is trying to authenticate against an AD or LDAP identity store.

ACS supports the following AD or LDAP attribute types for multi-value attributes:

- String
- Integer
- IP Address

After you configure these multi-value attributes, you can use them in authorization profiles.

You can construct the following forms of conditions in access policies involving multiple value attributes:

- [Multiple value attribute] [operator] [Multiple value attribute]
- [Single value attribute] [operator] [Multiple value attribute]
- [Multiple value attribute] [operator] [Single value attribute]
- [Multiple value attribute] [operator] [Static value]

Operators for String-Type Multi-Value Attributes

ACS supports the following operators for String-type multi-value attributes:

- Equals
- Not Equals
- Starts with
- Ends with
- Contains
- Not contains

[Table 8-13](#) displays the results of the conditions when you use the above operators among the multi-value, single value, and static value attribute operands.

Table 8-13 *Results of the Operators Used Between the String Type Multi-Value Attributes*

Left Operand	Right Operand	Equals	Not Equals	Starts with	Ends with	Contains	Not Contains
Multi-value attribute	Multi-value attribute	True if all values in the left operand are equal to at least one value in the right operand.	True if no value in the left operand is equal to any value in the right operand.	True if at least one value in the left operand starts with all values in the right operand.	True if at least one value in the left operand ends with all values in the right operand.	True if at least one value in the left operand contains all values in the right operand.	True if no value in the left operand contains any value in the right operand.
Single value attribute	Multi-value attribute						
Multi-value attribute	Single value attribute						
Multi-value attribute	Static value	True if at least one value in the left operand is equal to the value in the right operand.	True if no value in the left operand is equal to the value in the right operand.	True if at least one value in the left operand starts with the value in the right operand.	True if at least one value in the left operand ends with the value in the right operand.	True if at least one value in the left operand contains the value in the right operand.	True if no value in the left operand contains the value in the right operand.

Examples

- Left attribute value = 11 **Equals** Right attribute value = {22,11,33}
Result = True
- Left attribute value = 11 **Equals** Right attribute value = {22,44}
Result = False
- Left attribute value = 11 **Not Equals** Right attribute value = {22,33,44}
Result = True
- Left attribute value = 11 **Not Contains** Right attribute value = {22,11,33}
Result = False
- Left attribute value = 123 **Contains** Right attribute value = {12,23}
Result = True

Operators for Integer-Type Multi-Value Attributes

ACS supports the following operators for Integer-type multi-value attributes:

- =
- !=
- >
- >=
- <
- <=

Table 8-14 displays the results of the conditions when you use the above operators among the multi-value, single value, and static value attribute operands.

Table 8-14 *Results of the Operators Used Between the Integer-Type Multi-Value Attributes*

Left Operand	Right Operand	=	!=	>	>=	<	<=
Multi-value attribute	Multi-value attribute	True if at least one value in the left operand is equal to one value in the right operand.	True if no value in the left operand is equal to any value in the right operand.	True if at least one value in the left operand is greater than one value in the right operand.	True if at least one value in the left operand is greater than or equal to one value in the right operand.	True if at least one value in the left operand is less than one value in the right operand.	True if at least one value in the left operand is less than or equal to one value in the right operand.
Single value attribute	Multi-value attribute						
Multi-value attribute	Single value attribute						
Multi-value attribute	Static value	True if at least one value in the left operand is equal to the value in the right operand.	True if no value in the left operand is equal to the value in the right operand.	True if at least one value in the left operand is greater than the value in the right operand.	True if at least one value in the left operand is greater than or equal to the value in the right operand.	True if at least one value in the left operand is less than the value in the right operand.	True if at least one value in the left operand is less than or equal to the value in the right operand.

Examples

- Left attribute value = {11,22,33} = Right attribute value = 11
Result = True
- Left attribute value = {11,22,33} != Right attribute value = 11
Result = False
- Left attribute value = {11,22,33} > Right attribute value = 11
Result = True
- Left attribute value = {11,22,33} < Right attribute value = 11
Result = False

Operators for IP-Address-Type Multi-Value Attributes

ACS supports the following operators for IP-Address type multi-value attributes:

- Equals
- Not Equals

[Table 8-15](#) displays the results of the conditions when you use the above operators among the multi-value, single value, and static value attribute operands.

Table 8-15 *Results of the Operators Used Between the IP-Address Type Multi-Value Attributes*

Left Operand	Right Operand	Equals	Not Equals
Multi-value attribute	Multi-value attribute	True if at least one value in the left operand is equal to one value in the right operand.	True if no value in the left operand is equal to any value in the right operand.
Single value attribute	Multi-value attribute		
Multi-value attribute	Single value attribute		
Multi-value attribute	Static value		

Related Topics

- [Attribute Retrieval for Authorization, page 8-56](#)
- [Boolean Attribute Support in Active Directory or LDAP, page 8-57](#)
- [Group Retrieval for Authorization, page 8-61](#)
- [Certificate Retrieval for EAP-TLS Authentication, page 8-61](#)

Group Retrieval for Authorization

ACS can retrieve user or machine groups from Active Directory after a successful authentication and also retrieve the user or machine group independent of authentication for authorization and group mapping purposes. You can use the AD group data in authorization and group mapping tables and introduce special conditions to match them against the retrieved groups.

Related Topics

- [Attribute Retrieval for Authorization, page 8-56](#)
- [Boolean Attribute Support in Active Directory or LDAP, page 8-57](#)
- [Multi-Value Attribute Support in AD or LDAP, page 8-58](#)
- [Certificate Retrieval for EAP-TLS Authentication, page 8-61](#)

Certificate Retrieval for EAP-TLS Authentication

ACS 5.8.1 supports certificate retrieval for user or machine authentication that uses EAP-TLS protocol. The user or machine record on AD includes a certificate attribute of binary data type. This can contain one or more certificates. ACS refers to this attribute as userCertificate and does not allow you to configure any other name for this attribute.

ACS retrieves this certificate for verifying the identity of the user or machine. The certificate authentication profile determines the field (SAN, CN, SSN, SAN-Email, SAN-DNS, or SAN-other name) to be used for retrieving the certificates.

After ACS retrieves the certificate, it performs a binary comparison of this certificate with the client certificate. When multiple certificates are received, ACS compares the certificates to check if one of them match. When a match is found, ACS grants the user or machine access to the network.

Related Topics

- [Concurrent Connection Management, page 8-62](#)
- [User and Machine Account Restrictions, page 8-62](#)
- [Machine Access Restrictions, page 8-62](#)

Concurrent Connection Management

After ACS connects to the AD domain, at startup, ACS creates a number of threads to be used by the AD identity store for improved performance. Each thread has its own connection.

Related Topics

- [User and Machine Account Restrictions, page 8-62](#)
- [Machine Access Restrictions, page 8-62](#)

User and Machine Account Restrictions

While authenticating or querying a user or a machine, ACS checks whether:

- The user account disabled
- The user locked out
- The user's account has expired
- The query run outside of the specified logon hours

If the user has one of these limitations, the *AD1::IdentityAccessRestricted* attribute on the AD dedicated dictionary is set to indicate that the user has restricted access. You can use this attribute in group mapping and authorization rules.

Related Topics

- [Machine Access Restrictions, page 8-62](#)
- [Distributed MAR Cache, page 8-64](#)
- [Dial-In Permissions, page 8-65](#)
- [Callback Options for Dial-In users, page 8-66](#)
- [Joining ACS to an AD Domain, page 8-67](#)

Machine Access Restrictions

MAR helps tying the results of machine authentication to user authentication and authorization process. The most common usage of MAR is to fail authentication of users whose host machine does not successfully authenticate. The MAR is effective for all authentication protocols.

MAR functionality is based on the following points:

- As a result of Machine Authentication, the machine's RADIUS `Calling-Station-ID` attribute (31) is cached as an evidence for later reference.
- Administrator can configure the time to live (TTL) of the above cache entries in the AD settings page.
- Administrator can enable or disable MAR from AD settings page. However for MAR to work the following limitations must be taken into account:
 - Machine authentication must be enabled in the authenticating protocol settings
 - The AAA client must send a value in the Internet Engineering Task Force (IETF) RADIUS `Calling-Station-Id` attribute (31).
 - ACS does not replicate the cache of `Calling-Station-Id` attribute values from successful machine authentications.

- ACS do not persevere the cache of `Calling-Station-Id` attribute. So the content is lost when ACS crashes unexpectedly. The content is not verified for consistency in case the administrator performs configuration changes that may effect machine authentication.
- When the user authenticates with either PEAP or EAP-FAST, against AD external ID store then ACS performs an additional action. It searches the cache for the users `Calling-Station-Id`. If it is found then **Was-Machine-Authenticated** attribute is set to true on the session context, otherwise set to false.

**Note**

When you perform Machine Authentication using EAP-TLS protocol, you should enable the “Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory” option and select the appropriate LDAP or Active Directory in the **Certificate Authentication Profile > CN User Name > Edit Page**.

- For the above to function correctly, the user authentication request should contain the `Calling-Station-Id`. In case it does not, the **Was-Machine-Authenticated** attribute shall be set to false.
- The administrator can add rules to authorization policies that are based on AD GM attribute and on Machine authentication required attribute. Any rule that contains these two attributes will only apply if the following conditions are met:
 - MAR feature is enabled
 - Machine authentication in the authenticating protocol settings is enabled
 - External ID store is AD
- When a rule such as the one described above is evaluated, the attributes of AD GM and **Was-Machine-Authenticated** are fetched from the session context and checked against the rule's condition. According to the results of this evaluation an authorization result is set.
- Exemption list functionality is supported implicitly (in contrast to ACS 4.x). To exempt a given user group from the MAR the administrator can set a rule such that the column of **AD Group** consists of the group to exempt and the column of **Machine Authentication Required** consists of *No*. See the second rule in the table below for an example.

For example, the administrator will add rules to the authorization policy as follows:

AD Group	Machine Authentication Required	...	ATZ profile
Engineers	Yes	...	VLAN X
Managers	No	...	VLAN B
...	DENY ACCESS

The Engineers' rule is an example of MAR rule that only allows engineers access if their machine was successfully authenticated against windows DB.

The Managers' rule is an example of an exemption from MAR.

Related Topics

- [Distributed MAR Cache, page 8-64](#)
- [Dial-In Permissions, page 8-65](#)
- [Callback Options for Dial-In users, page 8-66](#)

- [Joining ACS to an AD Domain, page 8-67](#)

Distributed MAR Cache

ACS 5.8.1 supports the Machine Access Restriction cache per ACS deployment. That is, machine authentication results can be cached among the nodes within a deployment.

MAR Cache Distribution Groups

ACS 5.8.1 has the option to group ACS nodes in MAR cache distribution groups. This option is used to control the impact of MAR cache distribution operations on ACS performance and memory usage.

A text label is assigned to each ACS node, which is called the MAR cache distribution group value. ACS nodes are grouped based on the MAR cache distribution group value. You can perform MAR cache distribution operations only between the ACS nodes that are assigned to the same MAR cache distribution group.

If the group value of an ACS node is empty, then it is considered as not assigned to any MAR cache distribution group. Such ACS nodes are not part of any MAR cache distribution operations.

Distributed MAR Cache Operation

The ACS runtime component combines two operations to implement a distributed MAR cache:

- MAR cache replication with no guaranteed delivery
- MAR cache distributed search

MAR Cache Replication

The ACS runtime component stores a MAR entry, `authenticated Calling-Station-ID`, in a MAR cache during machine authentication. Initially, ACS saves the MAR entry in the local MAR cache. Then, the ACS runtime component replicates the MAR entry to the ACS nodes that belong to the same MAR cache distribution group.

The replication is performed based on the cache entry replication attempts and the cache entry replication time-outs that are configured in the ACS web interface.

The replication operation is performed in the background and does not interrupt or delay the user authentication that triggered this replication.

MAR Cache Distributed Search

When an authentication request comes in, ACS searches for the MAR entry in the local MAR cache. If a MAR entry is not found in the local MAR cache, then ACS queries the ACS nodes that are assigned to the same MAR cache distribution group.

The distributed search is performed based on the cache entry query attempts and cache entry query time-outs that are configured in the ACS web interface. The MAR entry search is also delayed until the first successful response from any of the queried ACS nodes, up to the maximum of the configured cache entry query timeout period. You can see any of the following messages in ACS View for an authentication that involves querying the MAR Cache:

- 24422 - ACS has confirmed previous successful machine authentication for user in Active Directory.
- 24423 - ACS has not been able to confirm previous successful machine authentication for user in Active Directory.
- 24701 - ACS peer has confirmed previous successful machine authentication for user in Active Directory.

- 24702 - ACS peers have not confirmed previous successful machine authentication for user in Active Directory.

Distributed MAR Cache Reliability

The ACS runtime component provides a reliable mechanism to implement the distributed MAR cache operation.

The distributed search option provides a fallback facility when the replication messages for some reason are not delivered. In this case, you can find the MAR cache entry on the ACS node that performs the machine authentication or on any one of the ACS nodes from the same MAR cache distribution group. The distributed search option also provides a fallback facility when the ACS node that performs the machine authentication is restarted. In this case, also, you can find the MAR cache entry in any one of the ACS nodes from the same MAR cache distribution group.

Distributed MAR Cache Persistency

ACS 5.8.1 stores the MAR cache content, calling-station-ID list, and the corresponding time stamps to a file on its local disk when you manually stop the ACS run-time services. The other ACS instances in the MAR cache distribution group cannot access the MAR cache of an ACS instance when the run-time services of this ACS instance are down. ACS does not store the MAR cache entries of an instance when there is an accidental restart of its run-time services.

ACS reads the MAR cache entries from the file on its local disk based on the cache entry time to live when the ACS run-time services get restarted. When the run-time services of an ACS instance come up after a restart, ACS compares the current time of that instance with the MAR cache entry time. If the difference between the current time and the MAR entry time is greater than the MAR cache entry time to live, then ACS does not retrieve that entry from disk. Otherwise, ACS retrieves that MAR cache entry and updates its MAR cache entry time to live.

Related Topics

- [Dial-In Permissions, page 8-65](#)
- [Callback Options for Dial-In users, page 8-66](#)
- [Joining ACS to an AD Domain, page 8-67](#)

Dial-In Permissions

The dial-in permissions of a user are checked during authentications or queries from Active Directory. The dial-in check is supported only for user authentications and not for machines, in the following authentication protocols:

- PAP
- MSCHAPv2
- EAP-FAST
- PEAP
- EAP-TLS.

The following results are possible:

- Allow Access
- Deny Access

- Control Access through Remote Access Policy. This option is only available for Windows 2000 native domain, Windows server 2003 domain.
- Control Access through NPS Network Policy. This is the default result. This option is only available for Windows server 2008, Windows 2008 R2, and Windows 2012 domains.

Related Topics

- [Callback Options for Dial-In users, page 8-66](#)
- [Joining ACS to an AD Domain, page 8-67](#)

Callback Options for Dial-In users

If the callback option is enabled, the server calls the caller back during the connection process. The phone number that is used by the server is set either by the caller or the network administrator.

The possible callback options are:

- No callback
- Set by Caller (routing and remote access service only). This option can be used to define a series of static IP routes that are added to the routing table of the server running the Routing and Remote Access service when a connection is made.
- Always callback to (with an option to set a number). This option can be used to assign a specific IP address to a user when a connection is made

The callback attributes should be returned on the RADIUS response to the device.

Dial-In Support Attributes

The user attributes on Active Directory are supported on the following servers:

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

ACS does not support Dial-in users on Windows 2000.

ACS Response

If you enable the dial-in check on ACS Active Directory and the user's dial-in option is 'Deny Access' on Active Directory, the authentication request is rejected with a message in the log, indicating that dial-in access is denied. If a user fails an MSCHAP v1/v2 authentication if the dial-in is not enabled, ACS should set on the EAP response a proper error code (NT error = 649).

In case that the callback options are enabled, the ACS RADIUS response contains the returned Service Type and Callback Number attributes as follows:

- If callback option is Set by Caller or Always Callback To, the service-type attribute should be queried on Active Directory during the user authentication. The service-type can be the following:
 - 3 = Callback Login
 - 4 = Callback Framed

- 9 = Callback NAS Prompt

This attribute should be returned to the device on Service-type RADIUS attribute. If ACS is already configured to return service-type attribute on the RADIUS response, the service-type value queried for the user on Active Directory replaces it.

- If the Callback option is Always Callback To, the callback number should also be queried on the Active Directory user. This value is set on the RADIUS response on the Cisco-AV-Pair attribute with the following values:
 - cisco-av-pair=lcp:callback-dialstring=[callback number value]
 - cisco-av-pair=Shell:callback-dialstring=[callback number value]
 - cisco-av-pair=Slip:callback-dialstring=[callback number value]
 - cisco-av-pair=Arap:callback-dialstring=[callback number value]

The callback number value is also returned on the RADIUS response, using the RADIUS attribute CallbackNumber (#19).

- If callback option is Set by Caller, the RADIUS response contains the following attributes with no value:
 - cisco-av-pair=lcp:callback-dialstring=
 - cisco-av-pair=Shell:callback-dialstring=
 - cisco-av-pair=Slip:callback-dialstring=
 - cisco-av-pair=Arap:callback-dialstring=

Related Topics

- [Joining ACS to an AD Domain, page 8-67](#)
- [Configuring an AD Identity Store, page 8-68](#)

Joining ACS to an AD Domain

You can join the ACS nodes from same deployment to different AD domains that has two way trust between each other. However, each node can be joined to a single AD domain. The policy definitions of those ACS nodes are not changed and that uses the same AD identity store.



Note

- Previous releases of ACS disconnects the Active Directory domain and displays the status as “joined but disconnected” in the Active Directory connection details page, when you stop the ad-client process manually from ACS CLI. But in ACS 5.8.1, when you stop the ad-client process manually from ACS CLI, ACS disconnects Active Directory domain and displays the status as “None” in Active Directory connection details page. If you start the ad-client process again from ACS CLI, ACS gets connected to the Active Directory domain and displays the status as “joined and connected” in AD connection details page.
- In ACS 5.8.1, you must manually join ACS to Active Directory after upgrading ACS 5.x to ACS 5.8.1. See [Installation and Upgrade Guide for Cisco Secure Access Control System](#) for more information on upgrade methods.
- Prior to Release 5.8.1, ACS started the adclient process only after joining the Active Directory domain to ACS. But, ACS 5.8.1 starts the adclient process soon after installing it.
- The Windows AD account, which joins ACS to the AD domain, can be placed in its own organizational unit (OU). It resides in its own OU either when the account is created or later on, with a restriction that the appliance name must match the name of the AD account.

- ACS does not support user authentication in AD when a user name is supplied with an alternative UPN suffix configured in OU level. The authentication works fine if the UPN suffix is configured in domain level.

For information on how to configure an AD identity store, see [Configuring an AD Identity Store, page 8-68](#).

Related Topics

- [Configuring an AD Identity Store, page 8-68](#)
- [Selecting an AD Group, page 8-73](#)
- [Configuring AD Attributes, page 8-74](#)
- [Configuring Machine Access Restrictions, page 8-76](#)

Configuring an AD Identity Store

The AD settings are not displayed by default, and they are not joined to an AD domain when you first install ACS. When you open the AD configuration page, you can see the list of all ACS nodes in the distributed deployment.

When you configure an AD identity store, ACS also creates the following:

- A new dictionary for that store with two attributes: the ExternalGroup attribute and another attribute for any attribute that is retrieved from the Directory Attributes page.
- A new attribute, IdentityAccessRestricted. You can manually create a custom condition for this attribute.
- A custom condition for group mapping from the ExternalGroup attribute—the custom condition name is AD1:ExternalGroups—and another custom condition for each attribute that is selected in the Directory Attributes page (for example, AD1:cn).

You can edit the predefined condition name, and you can create a custom condition from the Custom condition page. See [Creating, Duplicating, and Editing a Custom Session Condition, page 9-5](#).

To authenticate users and join ACS with an AD domain:

- Step 1** Choose **Users and Identity Stores > External Identity Stores > Active Directory**.

The Active Directory page appears.

The AD configuration page acts as a central AD management tool for all ACS nodes. You can perform the join and leave operations against a single ACS node or multiple ACS nodes on this page. You can also view the join results of all ACS nodes in the deployment at a single glance.

- Step 2** Modify the fields in the General tab as described in [Table 8-16](#).

Table 8-16 *Active Directory: General Page*

Option	Description
Connection Details	
Join	Click to join ACS with the AD domain for the given user, domain, and password entered. See Joining Nodes to an AD Domain, page 8-70 .

Table 8-16 Active Directory: General Page (continued)

Option	Description
Leave	Click to disconnect a single node or multiple nodes from the AD domain for the given user, domain, and password entered. See Disconnecting Nodes from the AD Domain , page 8-71.
End User Authentication Settings	
Enable password change	Click to allow the password to be changed.
Enable machine authentication	Click to allow machine authentication.
Enable dial-in check	Click to examine the user's dial-in permissions during authentication or query. The result of the check can cause a reject of the authentication in case the dial-in permission is denied. The result is not stored on the AD dictionary.
Enable callback check for dial-in clients	Click to examine the user's callback option during authentication or query. The result of the check is returned to the device on the RADIUS response. The result is not stored on the AD dictionary.
Use Kerberos for Plain Text	Click to use Kerberos for plain-text authentications. For ACS 5.8.1, the default and recommended option is MS-RPC. Until ACS 5.7, Kerberos was used as a default option.
Identity Resolution—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.	
If identity does not include the AD domain	
Reject the request	Click this option to reject the authentication request for users those who do not have any domain markups, such as a SAM name. This is useful in case of multi join domains where ACS 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	Click this option to search for the identity only in the trusted domains in the forest which are specified in the authentication domains section. This is the default option and identical to ACS 5.7 behavior for SAM account names.
Search in all the “Authentication Domains” section	Click this option to search for the identity in all authentication domains in all the trusted forests. This might increase latency and impact performance.
If some of the domains are unreachable	
Proceed with available domains	Click this option to proceed with the authentication if it finds a match in any of the available domains when a few domains are not reachable.
Drop the request	Click this option to drop the authentication request if the identity resolution encounters some unreachable or unavailable domains.

Step 3 Click:

- **Save Changes** to save the configuration.
- **Discard Changes** to discard all changes.
- If AD is already configured and you want to delete it, click **Clear Configuration** after you verify the following:
 - There are no policy rules that use custom conditions based on the AD dictionary.
 - The AD is not chosen as the identity source in any of the available access services.

- There are no identity store sequences with the AD.
- **Refresh** to update the data in Directory Groups, Authentication Domains, and Diagnostic Tool tabs after joining or leaving ACS to AD domain(s).

The Active Directory configuration is saved. The Active Directory page appears with the new configuration.

**Note**

- The AD configuration is affected (and sometimes gets disconnected) when there is a slow response from the server while you test the ACS connection with the AD domain. However the configuration works fine with the other applications.
- Active Directory page in ACS 5.8.1 is refreshed automatically for every 60 seconds. If you perform an operation in AD page, the status of the operation will be updated in AD page only after 60 seconds. If you want to see the updated status immediately, you must click **Refresh** option that is available at the bottom of the General tab.
- Due to NETBIOS limitations, ACS hostnames must contain less than or equal to 15 characters.

**Note**

If “User change password at next logon” option is enabled for an AD user:

- (a) If you use Kerberos for user authentication, the password gets changed immediately after you change the password on next login.
- (b) If you use MSRPC for user authentication, you must wait for a reasonable time for the new password to get synchronized with ACS after you change the password on next login. During this time, the old password may work. see <https://support.microsoft.com/en-us/kb/906305> for more information.

Joining Nodes to an AD Domain

You can join a single ACS node to only one AD domain. ACS does not support joining a single ACS node to multiple AD domains. But, ACS supports joining multiple ACS nodes to a single AD domain.

To join ACS nodes to an AD domain, complete the following steps:

- Step 1** Choose **Users and Identity Stores > External Identity Stores > Active Directory**.
The Active Directory page appears.
- Step 2** Select a single node or multiple nodes and click **Join**.
The Join page appears.
- Step 3** Complete the fields in the Join page as described in [Table 8-17](#).

Table 8-17 Join/Test Connection Page

Option	Description
Active Directory Domain Name	Name of the AD domain to which you want to join ACS.
Username	<p>Enter the username of a predefined AD user. An AD account which is required for the domain access in ACS, should have either of the following:</p> <ul style="list-style-type: none"> • Add workstations to the domain user in the corresponding domain. • Create Computer Objects or Delete Computer Objects permission on corresponding computers container where ACS machine's account is precreated (created before joining ACS machine to the domain). <p>Cisco recommends that you disable the lockout policy for the ACS account and configure the AD infrastructure to send alerts to the administrator if a wrong password is used for that account. This is because, if you enter a wrong password, ACS will not create or modify its machine account when it is necessary and therefore possibly deny all authentications.</p>
Password	Enter the user password. The password should have a minimum of 8 characters, using a combination of at least one lower case letter, one upper case letter, one numeral, and one special character. All special characters are supported.

Step 4 Click:

- **Join** to join the selected nodes to the AD domain. The status of the nodes are changed according to the join results.
- **Cancel** to cancel the connection.

**Note**

After joining ACS to an Active Directory domain, if you delete the name server from ACS CLI, ACS prompts you to restart the services. If you enter No for restarting the services, ACS does not restart its services and deletes the name server from the configuration. But in the Active Directory General page, ACS displays the status of the Active Directory domain as None.

Disconnecting Nodes from the AD Domain

To disconnect a single node or multiple nodes from an AD Domain, complete the following steps:

- Step 1** Choose **Users and Identity Stores > External Identity Stores > Active Directory**.
The Active Directory page appears.
- Step 2** Select a single node or multiple nodes and click **Leave**.
The Leave Connection page appears.
- Step 3** Complete the fields in the Leave Connection page as described in [Table 8-18](#).

Table 8-18 Leave Connection Page

Option	Description
Username	<p>Enter the username of a predefined AD user. An AD account which is required for the domain access in ACS, should have either of the following:</p> <ul style="list-style-type: none"> • Add workstations to the domain user in the corresponding domain. • Create Computer Objects or Delete Computer Objects permission on corresponding computers container where ACS machine's account is precreated (created before joining ACS machine to the domain). <p>Cisco recommends that you disable the lockout policy for the ACS account and configure the AD infrastructure to send alerts to the administrator if a wrong password is used for that account. This is because, if you enter a wrong password, ACS will not create or modify its machine account when it is necessary and therefore possibly deny all authentications.</p>
Password	Enter the user password.
Do not try to remove machine account	<p>Check this check box to disconnect the selected nodes from the AD domain, when you do not know the credentials or have any DNS issues.</p> <p>This operation disconnects the node from the AD domain and leaves an entry for this node in the database. Only administrators can remove this node entry from the database.</p>

Step 4 Click:

- **Leave** to disconnect the selected nodes from AD domain.
- **Cancel** to cancel the operation.

**Note**

- Administrators can perform operations the join or leave operations from the secondary server. When you perform these operations from the secondary server, it affects only the secondary server.
- Authentications are not obligated to fail immediately when you disable ACS account from Active Directory domain. Authentications can work as long as there are established connections or TGT tickets. Authentications can fail with different errors based on LDAP, Kerberos or RPC depends upon which connection it is using to connect to ACS. It also depends on replication between Domain Controllers.

Related Topics

- [Selecting an AD Group, page 8-73](#)
- [Configuring AD Attributes, page 8-74](#)
- [Configuring Machine Access Restrictions, page 8-76](#)
- [Advanced Tunning, page 8-77](#)
- [Configuring Authentication Domains, page 8-77](#)
- [Diagnose Active Directory Problems, page 8-78](#)
- [Active Directory Alarms and Reports, page 8-79](#)

Selecting an AD Group

Use this page to select groups that can then be available for policy conditions.

**Note**

To select groups and attributes from an AD, ACS must be connected to that AD.

- Step 1** Choose **Users and Identity Stores > External Identity Stores > Active Directory**, then click the **Directory Groups** tab.

The Groups page appears with corresponding Security Identifier (SID). The Selected Directory Groups field lists the AD groups you selected and saved. The AD groups you selected in the External User Groups page are listed and can be available as options in group mapping conditions in rule tables.

If you have more groups in other trusted domains or forests that are not displayed, you can use the search filter to narrow down your search results. You can also add a new AD group using the **Add** button.

**Note**

- ACS does not retrieve domain local groups. It is not recommended to use domain local groups in ACS policies. The reason is that the membership evaluation in domain local groups can be time consuming. So, by default, the domain local groups are not evaluated.
- ACS 5.5, 5.6, or 5.7 do not have SIDs associated with the directory groups. Therefore, after upgrading from ACS 5.5, 5.6, or 5.7 to ACS 5.8.1, the directory groups are displayed without the SID values. You can find a new column called SID against each directory groups and the value of SID will be empty for all the directory groups. You have to retrieve the directory groups again to set a SID value for the groups.

- Step 2** Click **Select** to see the available AD groups on the domain and its child domains. To see the AD trusted domain groups in the same forest, you need to explicitly provide the trusted domain details in the search base DN field.

The External User Groups dialog box appears displaying a list of AD groups in the domain, as well as other trusted domains in the same forest.

If you have more groups that are not displayed, use the search filter to refine your search and click **Go**.

- Step 3** Enter the AD groups or select them from the list, then click **OK**.

To remove an AD group from the list, click an AD group, then click **Deselect**.

- Step 4** Click:

- **Save Changes** to save the configuration.
- **Discard Changes** to discard all changes.
- If AD is already configured and you want to delete it, click **Clear Configuration** after you verify that there are no policy rules that use custom conditions based on the AD dictionary.

**Note**

- When configuring the AD Identity Store on ACS 5.x, the security groups defined on Active Directory are enumerated and can be used, but distribution groups are not shown. Active Directory Distribution groups are not security-enabled and can only be used with e-mail applications to send e-mail to collections of users. Please refer to Microsoft documentation for more information on distribution groups.
- Logon authentication may fail on Active Directory when ACS tries to authenticate users who belong to more than 1015 groups in external identity stores. This is due to the Local Security Authentication (LSA) limitations in Active Directory.

Related Topics

- [Configuring AD Attributes, page 8-74](#)
- [Configuring Machine Access Restrictions, page 8-76](#)
- [Advanced Tunning, page 8-77](#)
- [Configuring Authentication Domains, page 8-77](#)
- [Diagnose Active Directory Problems, page 8-78](#)
- [Active Directory Alarms and Reports, page 8-79](#)

Configuring AD Attributes

Use this page to select attributes that can then be available for policy conditions.

- Step 1** Choose **Users and Identity Stores > External Identity Stores > Active Directory**, then click the **Directory Attributes** tab.
- Step 2** Complete the fields in the Active Directory: Attributes page as described in [Table 8-19](#):

Table 8-19 *Active Directory: Attributes Page*

Option	Description
Name of example Subject to Select Attributes	Enter the name of a user or computer found on the joined domain. You can enter the user's or the computer's CN or distinguished name. The set of attributes that are displayed belong to the subject that you specify. The set of attributes are different for a user and a computer.
Select	Click to access the Attributes secondary window, which displays the attributes of the name you entered in the previous field.
Attribute Name List—Displays the attributes you have selected in the secondary Selected Attributes window. You can select multiple attributes together and submit them.	
Attribute Name	<ul style="list-style-type: none"> • Do one of the following: <ul style="list-style-type: none"> – Enter the name of the attribute. – You can also select an attribute from the list, then click Edit to edit the attribute. • Click Add to add an attribute to the Attribute Name list.

Table 8-19 Active Directory: Attributes Page (continued)

Option	Description
Type	Attribute types associated with the attribute names. Valid options are: <ul style="list-style-type: none"> String Integer 64 IP Address—This can be either an IPv4 or IPv6 address. Unsigned Integer 32 Boolean
Default	Specified attribute default value for the selected attribute: <ul style="list-style-type: none"> String—Name of the attribute. Integer 64—0 Unsigned Integer 64—0. IP Address—No default set. Boolean—No default set.
Policy Condition Name	Enter the custom condition name for this attribute. For example, if the custom condition name is AAA, enter AAA in this field and not AD1:att_name .
Select Attributes Secondary Window	Available from the Attributes secondary window only.
Search Filter	Specify a user or machine name. <ul style="list-style-type: none"> For user names, you can specify distinguished name, SAM, NetBios, or UPN format. For machine names, you can specify one of the following formats: MACHINE\$, NETBiosDomain\MACHINE\$, host/MACHINE, or host/machine.domain. You can specify non-English letters for user and machine names.
Attribute Name	The name of an attribute of the user or machine name you entered in the previous field.
Attribute Type	The type of attribute.
Attribute Value	The value of an attribute for the specified user or machine.

Step 3 Do one of the following:

- **Click Save Changes** to save the configuration.
- **Click Discard Changes** to discard all changes.
- If AD is already configured and you want to delete it, click **Clear Configuration** after you verify that there are no policy rules that use custom conditions based on the AD dictionary.

Related Topics

- [Configuring Machine Access Restrictions, page 8-76](#)
- [Advanced Tunning, page 8-77](#)
- [Configuring Authentication Domains, page 8-77](#)
- [Diagnose Active Directory Problems, page 8-78](#)
- [Active Directory Alarms and Reports, page 8-79](#)

Configuring Machine Access Restrictions

To configure the Machine Access Restrictions, complete the following steps:

- Step 1** Choose **Users and Identity Stores > External Identity Stores > Active Directory**, then click the **Machine Access Restrictions** tab.
- Step 2** Complete the fields in the Active Directory: Machine Access Restrictions page as described in [Table 8-20](#).

Table 8-20 *Active Directory: Machine Access Restrictions Page*

Option	Description
Enable Machine Access Restrictions	Check this check box to enable the Machine Access Restrictions controls in the web interface. This ensures that the machine authentication results are tied to user authentication and authorization. If you enable this feature, you must set the Aging time.
Aging time (hours)	Time after a machine was authenticated that a user can be authenticated from that machine. If this time elapses, user authentication fails. The default value is 6 hours. The valid range is from 1 to 8760 hours.
MAR Cache Distribution	
Cache entry replication timeout	Enter the time in seconds after which the cache entry replication gets timed out. The default value is 5 seconds. The valid range is from 1 to 10.
Cache entry replication attempts	Enter the number of times ACS has to perform MAR cache entry replication. The default value is 2. The valid range is from 0 to 5.
Cache entry query timeout	Enter the time in seconds after which the cache entry query gets timed out. The default value is 2 seconds. The valid range is from 1 to 10.
Cache entry query attempts	Enter the number of times that ACS has to perform the cache entry query. The default value is 1. The valid range is from 0 to 5.
Node	Lists all the nodes that are connected to this AD domain.
Cache Distribution Group	Enter the Cache Distribution Group of the selected node. This accepts any text string to a maximum of 64 characters. The Cache Distribution Group does not allow the special characters "(" and ")".

- Step 3** Do one of the following:
- **Click Save Changes** to save the configuration.
 - **Click Discard Changes** to discard all changes.
 - If AD is already configured and you want to delete it, click **Clear Configuration** after you verify that there are no policy rules that use custom conditions based on the AD dictionary.

Related Topics

- [Advanced Tunning, page 8-77](#)
- [Configuring Authentication Domains, page 8-77](#)
- [Diagnose Active Directory Problems, page 8-78](#)
- [Active Directory Alarms and Reports, page 8-79](#)

Advanced Tuning

The advanced tuning feature provides node-specific changes and settings to adjust the parameters deeper in the system. This page allows configuration of preferred Domain Controllers, Global Catalogs, Domain Controller failover parameters, and timeouts. This page also provide troubleshooting options like disable encryption. These settings are not intended for normal administration flow and should be used only under Cisco Support guidance.

Related Topics

- [Configuring Authentication Domains, page 8-77](#)
- [Diagnose Active Directory Problems, page 8-78](#)
- [Active Directory Alarms and Reports, page 8-79](#)

Configuring Authentication Domains

If you join ACS to an Active Directory domain, ACS has visibilities to other domains with which it has a trust relationship. By default, ACS permits authentication against all those trusted domains. You can restrict ACS to a subset of authentication domains while interacting with the Active Directory deployments. Configuring authentication domains enables you to select specific domains so that the authentications are performed against the selected domains only. Authentication domains improve security because they instruct ACS 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.

To configure Authentication Domains:

Before you Begin

Ensure that the ACS instance is joined to an Active Directory domain.

-
- | | |
|---------------|---|
| Step 1 | Choose Users and Identity Stores > External Identity Stores > Active Directory , then click the Authentication Domains tab.

A table appears with a list of your trusted domains. By default, ACS permits authentication against all trusted domains. |
| Step 2 | To allow only specified domains, check the check box next to the domains for which you want to allow authentication, and click Enable Selected . |
| Step 3 | Click Save Changes .

In the Authenticate column, the status of the selected domains are changed to Yes . |
-

Related Topics

- [Diagnose Active Directory Problems, page 8-78](#)
- [Active Directory Alarms and Reports, page 8-79](#)

Diagnose Active Directory Problems

The Diagnostic Tool is a service that runs on every ACS 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 ACS uses Active Directory.

There are multiple reasons for which ACS might be unable to join or authenticate against Active Directory. This tool helps ensure that the prerequisites for connecting ACS 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.

You can run the following three test without joining ACS to Active Directory to check if the Active Directory Daemon is running properly:

- System health - check AD service
- System health - check DNS configuration
- System health - check NTP

You can run the following available tests after joining ACS to Active Directory:

- DNS A record high level API query
- DNS A record low level API query
- DNS SRV record query
- DNS SRV record size
- LDAP test AD site association
- LDAP test DCs availability
- LDAP test DCs response time
- LDAP test - DC locator
- LDAP test - GC locator
- Kerberos test obtaining join point TGT
- Kerberos test bind and query to ROOT DSE
- Kerberos check SASL connectivity to AD

To diagnose Active Directory problems:

-
- Step 1** Choose **Users and Identity Stores > External Identity Stores > Active Directory**, then click the **Diagnostic Tools** tab.

The Diagnostic Tools tab displays the list of all available tests that you can run on ACS to check Active Directory domain functions.

- Step 2** Check the check box or check boxes next to the tests that you want to run.

- Step 3** Click:

- **Run Selected Tests** to run only the selected tests.
- **Run All Tests** to run all the tests.
- **Stop All Running Tests** to stop ACS from running all tests.

You can see the test results in **Result and Remedy** columns.

Related Topics

[Active Directory Alarms and Reports, page 8-79](#)

Active Directory Alarms and Reports

Alarms

ACS 5.8.1 introduced various alarms and reports to monitor and troubleshoot Active Directory related activities.

The following alarms are triggered for Active Directory errors and issues:

- Configured name server not available
- Joined domain is unavailable
- Authentication domain is unavailable
- Active Directory forest is unavailable
- AD Connector had to be restarted
- AD: ACS 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 RADIUS authentication and authorization. You can find this report here: **Launch Monitoring and Report Viewer > Monitoring and Reports > Reports > ACS Reports > AAA Protocol > RADIUS Authentications**.
- **TACACS+ Authentications Report**—This report shows detailed steps of the Active Directory TACACS+ authentication and authorization. You can find this report here: **Launch Monitoring and Report Viewer > Monitoring and Reports > Reports > ACS Reports > AAA Protocol > TACACS Authentications**.
- **AD Connector Operations Report**—The AD Connector Operations report provides a log of background operations performed by AD connector, such as ACS 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: **Launch Monitoring and Report Viewer > Monitoring and Reports > Reports > ACS Reports > ACS Instance > AD Connector Operations**.



Note

The first authentication of a user belongs to the large number of groups may fail with a timeout error. But, the subsequent authentications of the same user or another user belongs to the same group works properly.

Joining ACS to Domain Controllers

When ACS needs to connect to a domain controller or a global catalog, it sends SRV requests to the configured DNS servers to find out the available list of domain controllers for a domain and the global catalogs for a forest.

If the Active Directory configuration on ACS machine is assigned to a subnet, which in turn is assigned to a site, then ACS sends the DNS queries scoped to the site. That is the DNS server is supposed to return the domain controllers and the global catalogs serving that particular site to which the subnet is assigned to.

If the ACS machine is not assigned to a site, then ACS does not send the DNS queries scoped to the site. That is the DNS server is supposed to return all available domain controllers and global catalogs with no regard to the sites.

ACS iterates the available list of domain controllers or global catalogs and tries to establish the connection according to the order of the domain controllers or the global catalogs in the DNS response received from the DNS server.

Related Topics

- [RSA SecurID Server, page 8-80](#)
- [RADIUS Identity Stores, page 8-86](#)

RSA SecurID Server

ACS supports the RSA SecurID server as an external database. RSA SecurID two-factor authentication consists of the user's personal identification number (PIN) 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.

You can integrate with RSA SecurID authentication technology in any one of the following ways:

- Using the RSA SecurID agent—Users are authenticated with username and passcode through the RSA's native protocol.
- Using the RADIUS protocol—Users are authenticated with username and passcode through the RADIUS protocol.

RSA SecurID token server in ACS 5.8.1 integrates with the RSA SecurID authentication technology by using the RSA SecurID Agent.

Configuring RSA SecurID Agents

The RSA SecurID Server administrator can do the following:

- [Create an Agent Record \(sdconf.rec\), page 8-81](#)
- [Reset the Node Secret \(SecurID\), page 8-81](#)
- [Override Automatic Load Balancing, page 8-81](#)
- [Manually Intervene to Remove a Down RSA SecurID Server, page 8-81](#)
- [Passcode Caching, page 8-81](#)

Create an Agent Record (*sdconf.rec*)

To configure an RSA SecurID token server in ACS 5.8.1, the ACS administrator requires the *sdconf.rec* file. The *sdconf.rec* file is a configuration record file that specifies how the RSA agent communicates with the RSA SecurID server realm.

In order to create the *sdconf.rec* file, the RSA SecurID server administrator should add the ACS host as an Agent host on the RSA SecurID server and generate a configuration file for this agent host.

Reset the Node Secret (SecurID)

After the agent initially communicates with the RSA SecurID server, the server provides the agent with a node secret file called SecurID. Subsequent communication between the server and the agent relies on exchanging the node secret to verify the other's authenticity.

At times, you might have to reset the node secret. To reset the node secret:

- The RSA SecurID server administrator must uncheck the Node Secret Created check box on the Agent Host record in the RSA SecurID server.
- The ACS administrator must remove the SecurID file from ACS.

Override Automatic Load Balancing

RSA SecurID Agent automatically balances the requested loads on the RSA SecurID servers in the realm. However, you do have the option to manually balance the load. You can specify which server each of the agent hosts must use and assign a priority to each server so that the agent host directs authentication requests to some servers more frequently than others.

You must specify the priority settings in a text file and save it as *sdopts.rec*, which you can then upload to ACS.

Manually Intervene to Remove a Down RSA SecurID Server

When an RSA SecurID server is down, the automatic exclusion mechanism does not always work quickly. To speed up this process, you can remove the *sdstatus.12* file from ACS.

Passcode Caching

Passcode caching enables the user to perform more than one authentication with an RSA SecurID server using the same passcode.

ACS 5.8.1 stores users with passcode in a cache. User and passcode are entered into the cache after successful authentication with the RSA SecurID server. Upon authentication with the RSA SecurID server, ACS tries first to search for the authenticating user and passcode in the cache. If not found, ACS authenticates with the RSA SecurID server.

The passcode cache in ACS is available for a configurable amount of time from 1 to 300 seconds. The RSA SecurID server passcode entry in the cache is available for the amount of time that you configure. Within this period of time, the user can access the internet with the same passcode.

Creating and Editing RSA SecurID Token Servers

ACS 5.8.1 supports RSA SecurID Token Servers for authenticating users for the increased security that one-time passwords provide. RSA SecurID token servers provide two-factor authentication to ensure the authenticity of users.

To authenticate users against an RSA identity store, you must first create an RSA SecurID Token Server in ACS and configure the realm, ACS instance, and advanced settings.

ACS 5.8.1 supports only one RSA realm. You can configure the settings for the RSA realm. A single realm can contain many ACS instances.

**Note**

You must obtain the *sdconf.rec* file from the RSA SecurID server administrator and store it in ACS.

To create or edit an RSA SecurID token server:

-
- Step 1** Choose **Users and Identity Stores > External Identity Stores > RSA SecurID Token Servers**.
The RSA SecurID Token Servers page appears.
- Step 2** Click **Create**.
You can also click the identity store name that you want to modify, or check the box next to the name and click **Edit**.
- Step 3** Complete the fields in the RSA Realm Settings tab as described in [Table 8-21](#).

Table 8-21 *RSA Realm Settings Tab*

Option	Description
General	
Name	Name of the RSA realm.
Description	(Optional) The description of the RSA realm.
Server Connection	
Server Timeout <i>n</i> seconds	ACS waits for <i>n</i> seconds to connect to the RSA SecurID token server before timing out.
Reauthenticate on Change PIN	Check this check box to reauthenticate on change PIN.
Realm Configuration File	
Import new 'sdconf.rec' file	Click Browse to select the <i>sdconf.rec</i> file from your machine.
Node Secret Status	Once the user is first authenticated against RSA SecurID Token Server, the Node Secret Status is shown as <i>Created</i> .

- Step 4** Click the ACS Instance Settings tab. See [Configuring ACS Instance Settings, page 8-83](#) for more information.
- Step 5** Click the Advanced tab. See [Configuring Advanced Options, page 8-85](#) for more information.
- Step 6** Click **Submit** to create an RSA SecurID store.
The RSA SecurID Token Server page appears with the configured servers.
-

Related Topics:

- [RSA SecurID Server, page 8-80](#)
- [Configuring ACS Instance Settings, page 8-83](#)

- [Configuring Advanced Options, page 8-85](#)

Configuring ACS Instance Settings

The ACS Instance Settings tab appears with the current list of ACS instances that are active in the system. You cannot add or delete these entries. However, you can edit the available RSA Realm settings for each of these ACS instances.

[Table 8-22](#) describes the fields in the ACS Instance Settings tab.

Table 8-22 *ACS Instance Settings Tab*

Option	Description
ACS Instance	Name of the ACS instance.
Options File	Name of the options file.
Node Secret Status	Status of Node Secret. This can be one of the following: <ul style="list-style-type: none">• Created• Not created

You can edit the settings of the ACS instances that are listed on this page. To do this:

-
- Step 1** Check the check box next to the ACS instance that you want to edit and click **Edit**.
- The ACS instance settings dialog box appears. This dialog box contains the following tabs:
- RSA Options File—See [Editing ACS Instance Settings, page 8-83](#) for more information.
 - Reset Agents Files—See [Editing ACS Instance Settings, page 8-83](#) for more information.
- Step 2** Click **OK**.
-

Related Topics

- [RSA SecurID Server, page 8-80](#)
- [Creating and Editing RSA SecurID Token Servers, page 8-81](#)
- [Editing ACS Instance Settings, page 8-83](#)
- [Editing ACS Instance Settings, page 8-83](#)
- [Configuring Advanced Options, page 8-85](#)

Editing ACS Instance Settings

You can edit the ACS instance settings to:

- [Enable the RSA Options File, page 8-83](#)
- [Reset Agent Files, page 8-84](#)

Enable the RSA Options File

You can enable the RSA options file (*sdopts.rec*) on each ACS instance to control routing priorities for connections between the RSA agent and the RSA servers in the realm.

[Table 8-23](#) describes the fields in the RSA Options File tab.

Table 8-23 RSA Options File Tab

Option	Description
The RSA options file (sdopts.rec) may be enabled on each ACS instance to control the routing priorities for connections between the RSA agent and the RSA servers in the realm. For detailed description of the format of the sdopts.rec, please refer to the RSA Documentation.	
Use the Automatic Load Balancing status maintained by the RSA Agent	Choose this option to use the automatic load balancing status that the RSA agent maintains.
Override the Automatic Load Balancing status with the sdopts.rec file selected below	Choose this option to use the automatic load balancing status that is specified in the sdopts.rec file.
Current File	Lists the sdopts.rec file that is chosen currently.
Time stamp	Time when sdopts.rec file was last modified.
File Size	Size of the sdopts.rec file.
Import new 'sdopts.rec' file	Click Browse to import the new sdopts.rec file from your hard drive.
Note Changes will not take effect until the page which launched this popup is submitted.	

Do one of the following:

- Click **OK** to save the configuration.
- Click the **Reset Agent Files** tab to reset the secret key information or the status of active and inactive servers in the realm.

Related Topics

- [RSA SecurID Server, page 8-80](#)
- [Creating and Editing RSA SecurID Token Servers, page 8-81](#)
- [Configuring ACS Instance Settings, page 8-83](#)
- [Editing ACS Instance Settings, page 8-83](#)
- [Configuring Advanced Options, page 8-85](#)

Reset Agent Files

Use this page to reset the following:

- Node Secret key file, to ensure that communication with the RSA servers is encrypted.
- Status of the servers in the realm.

Step 1 Choose either of the following options:

- To reset node secret on the agent host, check the **Remove secure id file on submit** check box.
If you reset the node secret on the agent host, you must reset the agent host's node secret in the RSA server.
- To reset the status of servers in the realm, check the **Remove sdstatus.12 file on submit** check box.

Step 2 Click **OK**.

Related Topics

- [RSA SecurID Server, page 8-80](#)
- [Creating and Editing RSA SecurID Token Servers, page 8-81](#)
- [Configuring ACS Instance Settings, page 8-83](#)
- [Editing ACS Instance Settings, page 8-83](#)
- [Configuring Advanced Options, page 8-85](#)

Configuring Advanced Options

Use this page to do the following:

- Define what an access reject from an RSA SecurID token server means to you.
- Enable identity caching—Caching users in RSA is similar to caching users in RADIUS token with the logic and the purpose of the caching being the same. The only difference is that in RSA there is no attribute retrieval for users and therefore no caching of attributes. The user who is authenticated is cached, but without any attributes.
- Enable passcode caching—This option stores the passcodes after the first successful authentication with an RSA secure ID token server and uses the cached user credentials for the subsequent authentications if they happens within the configured time period.

To configure advanced options for the RSA realm:

-
- | | |
|---------------|--|
| Step 1 | Do one of the following: <ul style="list-style-type: none">• Click the Treat Rejects as Authentication failed radio button—ACS interprets this as an authentication reject from an RSA SecurID store and consider this as an authentication failure.• Click the Treat Rejects as User not found radio button—ACS interprets this as an authentication reject from an RSA SecurID store and consider this as “user not found.” |
| Step 2 | Check the Enable identity caching check box. <p>Enable identity caching to allow ACS to process requests that are not authenticated through the RSA server.</p> <p>The results obtained from the last successful authentication are available in the cache for the specified time period.</p> |
| Step 3 | Enter the aging time in minutes. <p>The identity cache stores the results of a successful login only for the time period specified here. The default value is 120 minutes. The valid range is from 1 to 1440 minutes.</p> |
| Step 4 | Check the Enable passcode caching check box. <p>Enable passcode caching to allow ACS to cache the passcodes and allow users to access the network with the same passcode for the specified time period.</p> |
| Step 5 | Enter the aging time in seconds. <p>The passcode cache stores the results of a successful login only for the time period specified here. The default value is 30 seconds. The valid range is from 1 to 300 seconds.</p> |
| Step 6 | Click Submit . |
-

**Note**

ACS displays the “InvalidPassword” error message in ACS view for the following scenarios when you authenticate users and administrators against RSA Identity Server and RSA SecurID Server as an external identity source:

- 1) Invalid Password is entered
- 2) User is disabled in external identity store
- 3) User does not exist in the external identity store

Related Topics

- [RSA SecurID Server, page 8-80](#)
- [Creating and Editing RSA SecurID Token Servers, page 8-81](#)
- [Configuring ACS Instance Settings, page 8-83](#)
- [Editing ACS Instance Settings, page 8-83](#)
- [Configuring Advanced Options, page 8-85](#)

RADIUS Identity Stores

RADIUS server is a third-party server that supports the RADIUS interface. RADIUS identity store, which is part of ACS, connects to the RADIUS server.

RADIUS servers are servers that come with a standard RADIUS interface built into them and other servers that support the RADIUS interface. ACS 5.8.1 supports any RADIUS RFC 2865-compliant server as an external identity store. ACS 5.8.1 supports multiple RADIUS token server identities.

For example, the RSA SecurID server and SafeWord server. RADIUS identity stores can work with any RADIUS Token server that is used to authenticate the user. RADIUS identity stores use the UDP port for authentication sessions. The same UDP port is used for all RADIUS communication.

**Note**

For ACS to successfully send RADIUS messages to a RADIUS-enabled server, you must ensure that the gateway devices between the RADIUS-enabled server and ACS allow communication over the UDP port. You can configure the UDP port through the ACS web interface.

This section contains the following topics:

- [Supported Authentication Protocols, page 8-87](#)
- [Failover, page 8-87](#)
- [Password Prompt, page 8-87](#)
- [User Group Mapping, page 8-87](#)
- [Groups and Attributes Mapping, page 8-87](#)
- [RADIUS Identity Store in Identity Sequence, page 8-88](#)
- [Authentication Failure Messages, page 8-88](#)
- [Username Special Format with Safeword Server, page 8-89](#)
- [User Attribute Cache, page 8-89](#)
- [Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-90](#)

Supported Authentication Protocols

ACS supports the following authentication protocols for RADIUS identity stores:

- RADIUS PAP
- TACACS+ ASCII/PAP
- PEAP with inner EAP-GTC
- EAP-FAST with inner EAP-GTC

Failover

ACS 5.8.1 allows you to configure multiple RADIUS identity stores. Each RADIUS identity store can have primary and secondary RADIUS servers. When ACS is unable to connect to the primary server, it uses the secondary server.

Password Prompt

RADIUS identity stores allow you to configure the password prompt. You can configure the password prompt through the ACS web interface.

User Group Mapping

To provide the per-user group mapping feature available in ACS 4.x, ACS 5.8.1 uses the attribute retrieval and authorization mechanism for users that are authenticated with a RADIUS identity store.

For this, you must configure the RADIUS identity store to return authentication responses that contain the [009\001] cisco-av-pair attribute with the following value:

ACS:CiscoSecure-Group-Id= N , where N can be any ACS group number from 0 through 499 that ACS assigns to the user.

Then, this attribute is available in the policy configuration pages of the ACS web interface while creating authorization and group mapping rules.

Groups and Attributes Mapping

You can use the RADIUS attributes retrieved during authentication against the RADIUS identity store in ACS policy conditions for authorization and group mapping. You can select the attributes that you want to use in policy conditions while configuring the RADIUS identity store. These attributes are kept in the RADIUS identity store dedicated dictionary and can be used to define policy conditions.



Note

You cannot query the RADIUS server for the requested attributes. You can only configure the RADIUS identity store to return the requested attributes. These attributes are available in the Access-Accept response as part of the attributes list.

You can use the attribute subscription feature of ACS 5.8.1 to receive RADIUS identity store attributes can on the ACS response to the device. The following RADIUS attributes are returned:

- Attributes that are listed in the RADIUS RFS
- Vendor-specific attributes

The following attribute types are supported:

- String
- Unsigned Integer
- IP Address
- Enumeration

If an attribute with multiple values is returned, the value is ignored, and if a default value has been configured, that value is returned. However, this attribute is reported in the customer log as a problematic attribute.

RADIUS Identity Store in Identity Sequence

You can add the RADIUS identity store for authentication sequence in an identity sequence. However, you cannot add the RADIUS identity store for attribute retrieval sequence because you cannot query the RADIUS identity store without authentication. ACS cannot distinguish between different error cases while authenticating with a RADIUS server.

RADIUS servers return an Access-Reject message for all error cases. 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.

You can, however, enable the Treat Rejects as Authentication Failure or User Not Found option available in the RADIUS identity store pages of the ACS web interface.

Authentication Failure Messages

When a user is not found in the RADIUS server, the RADIUS server returns an Access-Reject message. ACS provides you the option to configure this message through the ACS web interface as either Authentication Failed or Unknown User.

However, this option returns an Unknown User message not only for cases where the user is not known, but for all failure cases.

[Table 8-24](#) lists the different failure cases that are possible with RADIUS identity servers.

Table 8-24 Error Handling

Cause of Authentication Failure	Failure Cases
Authentication Failed	<ul style="list-style-type: none"> • User is unknown. • User attempts to login with wrong passcode. • User logon hours expired.

Table 8-24 *Error Handling*

Cause of Authentication Failure	Failure Cases
Process Failed	<ul style="list-style-type: none"> • RADIUS server is configured incorrectly in ACS. • 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.

Username Special Format with Safeword Server

Safeword token server supports authentication with the following username format:

Username—Username, OTP

ACS parses the username and converts this to:

Username—Username

Safeword token servers support both the formats. ACS works with various token servers. While configuring a Safeword server, you must check the Safeword Server check box for ACS to parse the username and convert it to the specified format.

This conversion is done in the RADIUS token server identity store before the request is sent to the RADIUS token server.

User Attribute Cache

RADIUS token servers, by default, do not support user lookups. However, the user lookup functionality is essential for the following ACS features:

- PEAP session resume—Happens after successful authentication during EAP session establishment
- EAP/FAST fast reconnect—Happens after successful authentication during EAP session establishment
- T+ Authorization—Happens after successful T+ Authentication

ACS 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 ACS nodes in a distributed deployment. You can configure the time to live (TTL) limit for the cache through the ACS web interface. 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.

Passcode Caching

Passcode caching enables the user to perform more than one authentication with an RADIUS identity server using the same passcode.

ACS 5.8.1 stores users with passcode in a cache. User and passcode are entered into the cache after successful authentication with the RADIUS Identity Server. Upon authentication with the RADIUS identity server, ACS tries first to search for the authenticating user and passcode in the cache. If not found, ACS authenticates with the RADIUS identity server.

The passcode cache in ACS is available for a configurable amount of time from 1 to 300 seconds. The RADIUS identity server passcode entry in the cache is available for the amount of time that you configure. Within this period of time, the user can access the internet with the same passcode.

Creating, Duplicating, and Editing RADIUS Identity Servers

ACS 5.8.1 supports the RADIUS identity server as an external identity store for the increased security that one-time passwords provide. RADIUS identity servers provide two-factor authentication to ensure the authenticity of the users.

To authenticate users against a RADIUS identity store, you must first create the RADIUS identity server in ACS and configure the settings for the RADIUS identity store. ACS 5.8.1 supports the following authentication protocols:

- RADIUS PAP
- TACACS+ ASCII/PAP
- PEAP with inner EAP-GTC
- EAP-FAST with inner EAP-GTC

For a successful authentication with a RADIUS identity server, ensure that:

- The gateway devices between the RADIUS identity server and ACS allow communication over the UDP port.
- The shared secret that you configure for the RADIUS identity server on the ACS web interface is identical to the shared secret configured on the RADIUS identity server.

To create, duplicate, or edit a RADIUS Identity Server:

-
- Step 1** Choose **Users and Identity Stores > External Identity Stores > RADIUS Identity Servers**. The RADIUS Identity Servers page appears with a list of RADIUS external identity servers.
- Step 2** Click **Create**. You can also:
- Check the check box next to the identity store you want to duplicate, then click **Duplicate**.
 - Click the identity store name that you want to modify, or check the box next to the name and click **Edit**.
- Step 3** Complete the fields in the General tab. See [Configuring General Settings, page 8-91](#) for a description of the fields in the General tab.
- Step 4** You can:
- Click **Submit** to save the RADIUS Identity Server.
 - Click the Shell Prompts tab. See [Configuring Shell Prompts, page 8-92](#) for a description of the fields in the Shell Prompts tab.
 - Click the Directory Attributes tab. See [Configuring Directory Attributes, page 8-93](#) for a description of the fields in the Directory Attributes tab.
 - Click the Advanced tab. See [Configuring Advanced Options, page 8-94](#) for a description of the fields in the Advanced tab.

Step 5 Click **Submit** to save the changes.

Related Topics

- [RADIUS Identity Stores, page 8-86](#)
- [Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-90](#)

Configuring General Settings

[Table 8-25](#) describes the fields in the General tab of the RADIUS Identity Servers page.

Table 8-25 *RADIUS Identity Server - General Tab*

Option	Description
Name	Name of the external RADIUS identity server.
Description	(Optional) A brief description of the RADIUS identity server.
SafeWord Server	Check this check box to enable a two-factor authentication using a SafeWord server.
Server Connection	
Enable Secondary Server	<p>Check this check box to use a secondary RADIUS identity server as a backup server in case the primary RADIUS identity server fails.</p> <p>If you enable the secondary server, you must configure the parameters for the secondary RADIUS identity server and must choose one of the following options:</p> <ul style="list-style-type: none"> • Always Access Primary Server First—Select this option to ensure that ACS always accesses the primary RADIUS identity server first before the secondary server is accessed. • Failback To Primary Server After <i>n</i> Minutes—Select this option to set the number of minutes ACS can use the secondary server for authentication. <p>After this time expires, ACS should again attempt to authenticate using the primary server. The default value is 5 minutes.</p>
Primary Server	
Server IP Address	IP address of the primary RADIUS identity server.
Shared Secret	<p>Shared secret between ACS and the primary RADIUS identity server.</p> <p>A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.</p>
Authentication Port	Port number on which the RADIUS primary server listens. Valid options are from 1 to 65,535. The default value is 1812.
Server Timeout <i>n</i> Seconds	Number of seconds, <i>n</i> , that ACS waits for a response from the primary RADIUS identity server before it determines that the connection to the primary server has failed. Valid options are from 1 to 300. The default value is 5.

Table 8-25 RADIUS Identity Server - General Tab (continued)

Option	Description
Connection Attempts	Specifies the number of times that ACS should attempt to reconnect before contacting the secondary RADIUS identity server or dropping the connection if no secondary server is configured. Valid options are from 1 to 10. The default value is 3.
Secondary Server	
Server IP Address	IP address of the secondary RADIUS identity server.
Shared Secret	<p>Shared secret between ACS and the secondary RADIUS identity server. The shared secret must be identical to the shared secret that is configured on the RADIUS identity server.</p> <p>A shared secret is an expected string of text, which a user must provide before the network device authenticates a username and password. The connection is rejected until the user supplies the shared secret.</p>
Authentication Port	Port number on which the RADIUS secondary server listens. Valid options are from 1 to 65,535. The default value is 1812.
Server Timeout <i>n</i> Seconds	<p>Number of seconds, <i>n</i>, that ACS waits for a response from the secondary RADIUS identity server before it determines that the connection to the secondary server has failed.</p> <p>Valid options are from 1 to 300. The default value is 5.</p>
Connection Attempts	Specifies the number of times that ACS should attempt to reconnect before dropping the request. Valid options are from 1 to 10. The default value is 3.

Related Topics

- [RADIUS Identity Stores, page 8-86](#)
- [Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-90](#)
- [Configuring Shell Prompts, page 8-92](#)
- [Configuring Directory Attributes, page 8-93](#)
- [Configuring Advanced Options, page 8-94](#)

Configuring Shell Prompts

For TACACS+ ASCII authentication, ACS must return the password prompt to the user. RADIUS identity server supports this functionality by the password prompt option. ACS can use the prompt that you configure in the Shell Prompts page on the ACS web interface. If the prompt is empty, the user receives the default prompt that is configured under TACACS+ global settings.

When establishing a connection with a RADIUS identity server, the initial request packets may not have the password. You must request a password. You can use this page to define the prompt that is used to request the password. To do this:

-
- Step 1** Enter the text for the prompt in the Prompt field.
- Step 2** Do one of the following:
- Click **Submit** to configure the prompt for requesting the password.

- Click the Directory Attributes tab to define a list of attributes that you want to use in policy rule conditions. See [Configuring Directory Attributes, page 8-93](#) for more information.

Related Topics

- [RADIUS Identity Stores, page 8-86](#)
- [Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-90](#)
- [Configuring General Settings, page 8-91](#)
- [Configuring Directory Attributes, page 8-93](#)
- [Configuring Advanced Options, page 8-94](#)

Configuring Directory Attributes

When a RADIUS identity server responds to a request, RADIUS attributes are returned along with the response. You can make use of these RADIUS attributes in policy rules.

In the Directory Attributes tab, you can specify the RADIUS attributes that you use in policy rule conditions. ACS maintains a separate list of these attributes.

Step 1 Modify the fields in the Directory Attributes tab as described in [Table 8-26](#).

Table 8-26 *RADIUS Identity Servers - Directory Attributes Tab*

Option	Description
Attribute List	Use this section to create the attracted list to include in policy conditions. As you include each attribute, its name, type, default value, and policy condition name appear in the table. To: <ul style="list-style-type: none"> • Add a RADIUS attribute, fill in the fields below the table and click Add. • Edit a RADIUS attribute, select the appropriate row in the table and click Edit. The RADIUS attribute parameters appear in the fields below the table. Edit as required, then click Replace.
Dictionary Type	RADIUS dictionary type. Click the drop-down list box to select a RADIUS dictionary type.
RADIUS Attribute	Name of the RADIUS attribute. Click Select to choose the RADIUS attribute. This name is composed of two parts: The attribute name and an extension to support AV-pairs if the attribute selected is a Cisco AV-Pair. For example, for an attribute, cisco-av-pair with an AV-pair name some-avpair , ACS displays cisco-av-pair.some-avpair . IETF and vendor VSA attribute names contain an optional suffix, <i>-nnn</i> , where <i>nnn</i> is the ID of the attribute.
Type	RADIUS attribute type. Valid options are: <ul style="list-style-type: none"> • String • Unsigned Integer 32 • IPv4 address
Default	(Optional) A default value that can be used if the attribute is not available in the response from the RADIUS identity server. This value must be of the specified RADIUS attribute type.
Policy Condition Name	Specify the name of the custom policy condition that uses this attribute.

Step 2 Do either of the following:

- Click **Submit** to save your changes and return to the RADIUS Identity Servers page.
- Click the Advanced tab to configure failure message handling and to enable identity caching. See [Configuring Advanced Options, page 8-94](#) for more information.

Related Topics

- [RADIUS Identity Stores, page 8-86](#)
- [Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-90](#)
- [Configuring General Settings, page 8-91](#)
- [Configuring Shell Prompts, page 8-92](#)
- [Configuring Advanced Options, page 8-94](#)

Configuring Advanced Options

In the Advanced tab, you can do the following:

- Define what an access reject from a RADIUS identity server means to you.
- Enable identity caching.
- Enable passcode caching.

[Table 8-27](#) describes the fields in the Advanced tab of the RADIUS Identity Servers page.

Table 8-27 *RADIUS Identity Servers — Advanced Tab*

Option	Description
This Identity Store does not differentiate between 'authentication failed' and 'user not found' when an authentication attempt is rejected. From the options below, select how such an authentication reject from the Identity Store should be interpreted by ACS for Identity Policy processing and reporting.	
Treat Rejects as 'authentication failed'	Click this option to consider all ambiguous access reject attempts as failed authentications.
Treat Rejects as 'user not found'	Click this option to consider all ambiguous access reject attempts as unknown users.
Identity caching is used to allow processing of requests that do not perform authentication against the server. The cache retains the results and attributes retrieved from the last successful authentication for the subject.	
Enable identity caching	Check this check box to enable identity caching. If you enable identity caching, you must enter the time in minutes for which you want ACS to retain the identity cache.
Aging Time <i>n</i> Minutes	Enter the time in minutes for which you want ACS to retain the identity cache. Valid options are from 1 to 1440.
Enable passcode caching	Check this check box to enable passcode caching. If you enable passcode caching, you must enter the time in seconds for which you want ACS to retain the passcode cache.
Aging Time <i>n</i> Seconds	Enter the time in seconds for which you want ACS to retain the passcode cache. Valid options are from 1 to 300. The default value is 30 seconds.

Click **Submit** to save the RADIUS Identity Server.

Related Topics

- [RADIUS Identity Stores, page 8-86](#)
- [Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-90](#)

Configuring CA Certificates

When a client uses the EAP-TLS protocol to authenticate itself against the ACS server, it sends a client certificate that identifies itself to the server. To verify the identity and correctness of the client certificate, the server must have a preinstalled certificate from the Certificate Authority (CA) that has digitally signed the client certificate.

If ACS does not trust the client's CA certificate, then you must install in ACS the entire chain of successively signed CA certificates, all the way to the top-level CA certificate that ACS trusts. CA certificates are also known as trust certificates.

You use the CA options to install digital certificates to support EAP-TLS authentication. ACS uses the X.509 v3 digital certificate standard. ACS also supports manual certificate acquisition and provides the means for managing a certificate trust list (CTL) and certificate revocation lists (CRLs).

Digital certificates do not require the sharing of secrets or stored database credentials. They can be scaled and trusted over large deployments. If managed properly, they can serve as a method of authentication that is stronger and more secure than shared secret systems.

Mutual trust requires that ACS have an installed certificate that can be verified by end-user clients. This server certificate may be issued from a CA or, if you choose, may be a self-signed certificate. For more information, see [Configuring Local Server Certificates, page 18-16](#).



Note

ACS builds a certificate chain with the CA certificates that you add to it and uses this chain during TLS negotiations. You must add the certificate that signed the server certificate to the CA. You must ensure that the chain is signed correctly and that all the certificates are valid.

If the server certificate and the CA that signed the server certificate are installed on ACS, ACS sends the full certificate chain to the client.



Note

ACS does not support wildcard certificates.

Related Topics

- [Adding a Certificate Authority, page 8-95](#)
- [Editing a Certificate Authority and Configuring Certificate Revocation Lists, page 8-96](#)
- [Deleting a Certificate Authority, page 8-98](#)
- [Exporting a Certificate Authority, page 8-99](#)

Adding a Certificate Authority

The supported certificate formats are DER, PEM, or CER.

To add a trusted CA (Certificate Authority) certificate:

-
- Step 1** Choose **Users and Identity Stores > Certificate Authorities**.
The Trust Certificate page appears.
- Step 2** Click **Add**.
- Step 3** Complete the fields in the Certificate File to Import page as described in [Table 8-28](#):

Table 8-28 *Certificate Authority Properties Page*

Option	Description
Certificate File to Import	
Certificate File	Enter the name of the certificate file. Click Browse to navigate to the location on the client machine where the trust certificate is located.
Trust for client with EAP-TLS	Check this box so that ACS will use the certificate trust list for the EAP protocol.
Allow Duplicate Certificates	Allows you to add certificates with the same CN and SKI with different Valid From, Valid To, and Serial numbers.
Description	Enter a description of the CA certificate.

- Step 4** Click **Submit**.
The new certificate is saved. The Trust Certificate List page appears with the new certificate.
-

Related Topics

- [User Certificate Authentication, page C-6](#)
- [Overview of EAP-TLS, page C-6](#)

Editing a Certificate Authority and Configuring Certificate Revocation Lists

Use this page to edit a trusted CA (Certificate Authority) certificate.

-
- Step 1** Choose **Users and Identity Stores > Certificate Authorities**.
The Trust Certificate page appears with a list of configured certificates.
- Step 2** Click the name that you want to modify, or check the check box for the Name, and click **Edit**.
Complete the fields in the Edit Trust Certificate List Properties Page as described in [Table 8-29](#):
When ACS delays the CA CRL, the CA is retained on the local file system. The CA is not refreshed until you resubmit it.
By default ACS will fail all user certificates of a CA for which the CRL has expired.
- If the CA certificate is resubmitted, the following error is shown: `12514 EAP-TLS failed SSL/TLS handshake`. This is because of the unknown CA.
 - If the CA certificate is not resubmitted, the following error is shown: `12515 EAP-TLS failed SSL/TLS handshake`. This is because of the expired CRL.

If you choose Ignore CRL Expiration, ACS fails authentication for the revoked certificates and passes the authentication for non-revoked certificates.

Table 8-29 *Edit Certificate Authority Properties Page*

Option	Description
Issuer	
Friendly Name	The name that is associated with the certificate.
Description	(Optional) A brief description of the CA certificate.
Issued To	<i>Display only.</i> The entity to which the certificate is issued. The name that appears is from the certificate subject.
Issued By	<i>Display only.</i> The certification authority that issued the certificate.
Valid from	<i>Display only.</i> The start date of the certificate's validity. An X509 certificate is valid only from the start date to the end date (inclusive).
Valid To (Expiration)	<i>Display only.</i> The last date of the certificate's validity.
Serial Number	<i>Display only.</i> The serial number of the certificate.
Description	Description of the certificate.
Usage	
Trust for client with EAP-TLS	Check this box so that ACS will use the trust list for the TLS-related EAP protocols.
Certificate Status Validation	
OCSP Configuration	
Use this section to configure the OCSP service.	
Validate against OCSP service	Check this box and select the OCSP service from the drop-down list to validate the requests against the selected the OCSP service.
Reject the request if certificate status could not be determined by OCSP	Check this box to reject the request if the certificate status could not be determined by the OCSP service.
Certificate Revocation List Configuration	
Use this section to configure the CRL.	
Download CRL	Check this box to download the CRL.
CRL Distribution URL	Enter the CRL distribution URL. You can specify a URL that uses an HTTP or secure HTTPS connection. When you use a HTTPS URL, you must install the corresponding HTTPS server's CA certificate in ACS. You can configure a proxy server in ACS for CRL download so that ACS communicates with the CRL distribution server through the configured proxy server. For more information, see Configuring HTTP Proxy Settings for CRL Requests , page 18-3.
Retrieve CRL	ACS attempts to download a CRL from the CA. Toggle the time settings for ACS to retrieve a new CRL from the CA. <ul style="list-style-type: none"> Automatically—Obtain the next update time from the CRL file. If unsuccessful, ACS tries to retrieve the CRL periodically after the first failure until it succeeds. Every—Determines the frequency between retrieval attempts. Enter the amount in units of time.
If Download Failed Wait	Enter the amount of time to attempt to retrieve the CRL, if the retrieval initially failed.

Table 8-29 Edit Certificate Authority Properties Page (continued)

Option	Description
Bypass CRL Verification if CRL is not Received	If unchecked, all the client requests that use the certificate that is signed by the selected CA will be rejected until ACS receives the CRL file. When checked, the client request may be accepted before the CRL is received.
Ignore CRL Expiration	<p>Check this box to check a certificate against an outdated CRL.</p> <ul style="list-style-type: none"> When checked, ACS continues to use the expired CRL and permits or rejects EAP-TLS authentications according to the contents of the CRL. When unchecked, ACS examines the expiration date of the CRL in the Next Update field in the CRL file. If the CRL has expired, all authentications that use the certificate that is signed by the selected CA are rejected.

Step 3 Click **Submit**.

The Trust Certificate page appears with the edited certificate.

The administrator has the rights to configure CRL and OCSP verification. If both CRL and OCSP verification are configured at the same time, then ACS performs OCSP verification first. If it detects any communication problems with either the primary or secondary servers, or if the verification returns the status of a given certificate as unknown, then ACS moves on to perform the CRL validation.

Related Topics

- [User Certificate Authentication, page C-6](#)
- [Overview of EAP-TLS, page C-6](#)
- [Configuring HTTP Proxy Settings for CRL Requests, page 18-3](#)

Deleting a Certificate Authority

Use this page to delete a trusted CA (Certificate Authority) certificate:

Step 1 Choose **Users and Identity Stores > Certificate Authorities**.

The Trust Certificate List page appears with a list of configured certificates.

Step 2 Check one or more check boxes next to the certificates that you want to delete.**Step 3** Click **Delete**.**Step 4** Click **Yes** to confirm.

The Trust Certificate page appears without the deleted certificate(s).

Related Topic

- [Overview of EAP-TLS, page C-6](#)

Exporting a Certificate Authority

To export a trust certificate:

-
- | | |
|---------------|---|
| Step 1 | Choose Users and Identity Stores > Certificate Authorities .
The Trust Certificate List page appears with a list of configured certificates. |
| Step 2 | Check the box next to the certificates that you want to export. |
| Step 3 | Click Export .
This operation exports the trusted certificate to the client machine. |
| Step 4 | Click Yes to confirm.
You are prompted to install the exported certificate on your client machine. |
-

Related Topics

- [User Certificate Authentication, page C-6](#)
- [Overview of EAP-TLS, page C-6](#)

Configuring Certificate Authentication Profiles

The certificate authentication profile defines the X509 certificate information to be used for a certificate-based access request. You can select an attribute from the certificate to be used as the username.

You can select a subset of the certificate attributes to populate the username field for the context of the request. The username is then used to identify the user for the remainder of the request, including the identification used in the logs.

You can use the certificate authentication profile to retrieve certificate data to further validate a certificate presented by an LDAP or AD client. The username from the certificate authentication profile is used to query the LDAP or AD identity store.

ACS compares the client certificate against all certificates retrieved from the LDAP or AD identity store, one after another, to see if one of them matches. ACS either accepts or rejects the request.



Note

For ACS to accept a request, only one certificate from either the LDAP or the AD identity store must match the client certificate.

When ACS processes a certificate-based request for authentication, one of two things happens: the username from the certificate is compared to the username in ACS that is processing the request, or ACS uses the information that is defined in the selected LDAP or AD identity store to validate the certificate information.

You can duplicate a certificate authentication profile to create a new profile that is the same, or similar to, an existing certificate authentication profile. After duplication is complete, you access each profile (original and duplicated) separately, to edit or delete them.

ACS 5.8.1 now supports certificate name constraint extension. It accepts the client certificates whose issuers contain the name constraint extension. It checks the client certificates for CA and sub-CA certificates. This extension defines a name space for all subject names in the subsequent certificates in

a certificate path. It applies to both the subject distinguished name and the subject alternative name. These restrictions are applicable only when the specified name form is present in the client certificate. The ACS authentication fails if the client certificate is excluded or not permitted by the namespace.

Supported Name Constraints:

- Directory name
- DNS
- Email
- URL

Unsupported Name Constraints:

- IP address
- Other name

To create, duplicate, or edit a certificate authentication profile, complete the following steps:

Step 1 Choose **Users and Identity Stores > Certificate Authentication Profile**.

The Certificate Authentication Profile page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the certificate authentication profile that you want to duplicate, then click **Duplicate**.
- Click the certificate authentication profile that you want to modify, or check the check box next to the name and click **Edit**.

The Certificate Authentication Profile Properties page appears.

Step 3 Complete the fields in the Certificate Authentication Profile Properties page as described in [Table 8-30](#):

Table 8-30 *Certificate Authentication Profile Properties Page*

Option	Description
General	
Name	Enter the name of the certificate authentication profile.
Description	Enter a description of the certificate authentication profile.
Certificate Definition	

Table 8-30 Certificate Authentication Profile Properties Page (continued)

Option	Description
Principal Username X509 Attribute	Available set of principal username attributes for x509 authentication. The selection includes: <ul style="list-style-type: none">• Common Name• Subject Alternative Name• Subject Serial Number• Subject• Subject Alternative Name - Other Name• Subject Alternative Name - EMail• Subject Alternative Name - DNS
Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory	<p>Check this check box if you want to validate certificate information for authentication against a selected LDAP or AD identity store.</p> <p>If you select this option, you must enter the name of the LDAP or AD identity store, or click Select to select the LDAP or AD identity store from the available list.</p>

Step 4 Click **Submit**.

The Certificate Authentication Profile page reappears.

Related Topics

- [Viewing Identity Policies, page 10-23](#)
- [Configuring Identity Store Sequences, page 8-101](#)
- [Creating External LDAP Identity Stores, page 8-34](#)

Configuring Identity Store Sequences

An access service identity policy determines the identity sources that ACS uses for authentication and attribute retrieval. An identity source consists of a single identity store or multiple identity methods. When you use multiple identity methods, you must first define them in an identity store sequence, and then specify the identity store sequence in the identity policy.

An identity store sequence defines the sequence that is used for authentication and attribute retrieval and an optional additional sequence to retrieve additional attributes.

Authentication Sequence

An identity store sequence can contain a definition for certificate-based authentication or password-based authentication or both.

- If you select to perform authentication based on a certificate, you specify a single Certificate Authentication Profile, which you have already defined in ACS.
- If you select to perform authentication based on a password, you can define a list of databases to be accessed in sequence.

When authentication succeeds, any defined attributes within the database are retrieved. You must have defined the databases in ACS.

Attribute Retrieval Sequence

You can optionally define a list of databases from which to retrieve additional attributes. These databases can be accessed regardless of whether you use password or certificate-based authentication. When you use certificate-based authentication, ACS populates the username field from a certificate attribute and then uses the username to retrieve attributes.

ACS can retrieve attributes for a user, even when:

- The user's password is flagged for a mandatory change.
- The user's account is disabled.

When you perform password-based authentication, you can define the same identity database in the authentication list and the attribute retrieval list. However, if the database is used for authentication, it will not be accessed again as part of the attribute retrieval flow.

ACS authenticates a user or host in an identity store only when there is a single match for that user or host. If an external database contains multiple instances of the same user, authentication fails. Similarly, ACS retrieves attributes only when a single match for the user or host exists; otherwise, ACS skips attribute retrieval from that database.

This section contains the following topics:

- [Creating, Duplicating, and Editing Identity Store Sequences, page 8-102](#)
- [Deleting Identity Store Sequences, page 8-104](#)

Creating, Duplicating, and Editing Identity Store Sequences

To create, duplicate, or edit an identity store sequence:

Step 1 Choose **Users and Identity Stores > Identity Store Sequences**.

The Identity Store Sequences page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box next to the sequence that you want to duplicate, then click **Duplicate**.
- Click the sequence name that you want to modify, or check the check box next to the name and click **Edit**.

The Identity Store Sequence Properties page appears as described in [Table 8-31](#).

Table 8-31 *Identity Store Sequence Properties Page*

Option	Description
General	
Name	Enter the name of the identity store sequence.
Description	Enter a description of the identity store sequence.
Authentication Method List	
Certificate Based	Check this check box to use the certificate-based authentication method. If you choose this option, you must enter the certificate authentication profile. Click Select to choose the profile from a list of available profiles.

Table 8-31 Identity Store Sequence Properties Page (continued)

Option	Description
Password Based	<p>Check this check box to use the password-based authentication method. If you choose this option, you must choose the set of identity stores that ACS will access one after another until a match is found.</p> <p>If you choose this option, you must select a list of identity stores in the Authentication and Attribute Retrieval Search List area for ACS to access the identity stores one after another.</p>
Authentication and Attribute Retrieval Search List	
Note This section appears only when you check the Password Based option.	
Available	Available set of identity stores to access.
Selected	<p>Selected set of identity stores to access in sequence until first authentication succeeds. Use the Up and Down arrows at the right of the list to define the order of access.</p> <p>ACS automatically retrieves attributes from identity stores that you selected for authentication. You do not need to select the same identity stores for attribute retrieval.</p>
Additional Attribute Retrieval Search List	
Available	Available set of additional identity stores for attribute retrieval.
Selected	<p>(Optional) The selected set of additional identity stores for attribute retrieval. Use the Up and Down arrows at the right of the list to define the order of access.</p> <p>ACS automatically retrieves attributes from identity stores that you selected for authentication. You do not need to select the same identity stores for attribute retrieval.</p>
Internal User/Host	
If internal user/host is not found or disabled then exit the sequence and treat as User Not Found	<p>This option is applicable for the attribute phase and when the Internal Identity Store is in the Attribute retrieval list.</p> <p>ACS exists the sequence and treats it as User Not Found if this option is selected and the user not found or is disabled.</p>
Advanced Options	
Break sequence	<p>If this option is selected and if an authentication attempt against current Identity Store results in process error, the flow breaks the Identity Stores sequence. The flow then continues to the Fail-Open option configured in the Identity Policy.</p> <p>The same applies to attribute retrieval.</p>
Continue to next identity store in the sequence	<p>If this is checked and if authentication with the current Identity Store results in a process error, the flow tries to authenticate it with the next Identity Store in the authentication list.</p> <p>The same applies to attribute retrieval phase.</p>

Step 3 Click **Submit**.

The Identity Store Sequences page reappears.

Related Topics

- [Performing Bulk Operations for Network Resources and Users, page 7-8](#)
- [Viewing Identity Policies, page 10-23](#)
- [Managing Internal Identity Stores, page 8-4](#)

- [Managing External Identity Stores, page 8-29](#)
- [Configuring Certificate Authentication Profiles, page 8-99](#)
- [Deleting Identity Store Sequences, page 8-104](#)

Deleting Identity Store Sequences

To delete an identity store sequence:

Step 1 Choose **Users and Identity Stores > Identity Store Sequences**.

The Identity Store Sequences page appears with a list of your configured identity store sequences.

Step 2 Check one or more check boxes next to the identity store sequences that you want to delete.

Step 3 Click **Delete**.

The following error message appears:

Are you sure you want to delete the selected item/items?

Step 4 Click **OK**.

The Identity Store Sequences page appears, without the deleted identity store sequence(s) listed.

Related Topics

- [Performing Bulk Operations for Network Resources and Users, page 7-8](#)
- [Viewing Identity Policies, page 10-23](#)
- [Managing Internal Identity Stores, page 8-4](#)
- [Managing External Identity Stores, page 8-29](#)
- [Configuring Certificate Authentication Profiles, page 8-99](#)
- [Creating, Duplicating, and Editing Identity Store Sequences, page 8-102](#)



Managing Policy Elements

A policy defines the authentication and authorization processing of clients that attempt to access the ACS network. A client can be a user, a network device, or a user associated with a network device.

Policies are sets of rules. Rules contain policy elements, which are sets of conditions and results that are organized in rule tables. See [ACS 5.x Policy Model, page 3-1](#) for more information on policy design and how it is implemented in ACS.

Before you configure your policy rules, you must create the policy elements, which are the conditions and results to use in those policies. After you create the policy elements, you can use them in policy rules. See [Managing Access Policies, page 10-1](#) for more information on managing services, policies, and policy rules.

These topics contain.

- [Managing Policy Conditions, page 9-1](#)
- [Managing Authorizations and Permissions, page 9-17](#)
- [Creating, Duplicating, and Editing Downloadable ACLs, page 9-31](#)



Note

When Cisco Security Group Access license is installed, you can also configure Security Groups and Security Group Access Control Lists (SGACLs), which you can then use in Security Group Access authorization policies. For information about configuring security groups for Security Group Access, see [Creating Security Groups, page 4-23](#).

Managing Policy Conditions

You can configure the following items as conditions in a rule table:

- Request/Protocol Attributes—ACS retrieves these attributes from the authentication request that the user issues.
- Identity Attributes—These attributes are related to the identity of the user performing a request. These attributes can be retrieved from the user definition in the internal identity store or from user definitions that are stored in external identity stores, such as LDAP and AD.
- Identity Groups—ACS maintains a single identity group hierarchy that is used for all types of users and hosts. Each internal user or host definition can include an association to a single identity group within the hierarchy.

You can map users and hosts to identity groups by using the group mapping policy. You can include identity groups in conditions to configure common policy conditions for all users in the group. For more information about creating identity groups, see [Managing Identity Attributes, page 8-7](#).

- **Network Device Groups (NDGs)**—Devices issuing requests are included in one or more of up to 12 device hierarchies. You can include hierarchy elements in policy conditions. For more information about creating NDGs, see [Network Device Groups, page 7-1](#).
- **Date and Time Conditions**—You can create named conditions that define specific time intervals across specific days of the week. You can also associate expiry dates with date and time conditions.

A date and time condition is a condition that takes the current date and time and effectively returns either true or false to indicate whether or not the condition is met. There are two components within the date and time condition:

- **Enable Duration**—You have the option to limit the duration during which the condition is enabled by specifying an optional start time, end time, or both. This component allows you to create rules with limited time durations that effectively expire.

If the condition is not enabled, then this component of the date and time condition returns false.

- **Time Intervals**—On the ACS web interface, you see a grid of time that shows the days of the week and the hours within each day. Each cell in the grid represents one hour. You can either set or clear the cells.

If the date and time when a request is processed falls at a time when the corresponding time interval is set, then this component of the date and time condition returns true.

Both components of the date and time condition are considered while processing a request. The date and time condition is evaluated as true only if both components return a true value.

- **Network Conditions**—You can create filters of the following types to restrict access to the network:
 - **End Station Filters**—Based on end stations that initiate and terminate the connection. End stations may be identified by IP address, MAC address, calling line identification (CLI), or dialed number identification service (DNIS) fields obtained from the request.
 - **Network Device Filters**—Based on the AAA client that processes the request. A network device can be identified by its IP address, by the device name that is defined in the network device repository, or by the NDG.
 - **Device Port Filters**—Network device definition might be supplemented by the device port that the end station is associated with.

Each network device condition defines a list of objects that can then be included in policy conditions, resulting in a set of definitions that are matched against those presented in the request.

The operator that you use in the condition can be either *match*, in which case the value presented must match at least one entry within the network condition, or *no matches*, in which case it should not match any entry in the set of objects that is present in the filter.

You can include Protocol and Identity attributes in a condition by defining them in custom conditions or in compound conditions.

- **UserIsInManagementHierarchy**—This attribute returns true as a result when the management hierarchy defined for the user equals or contained in the network device's hierarchy. The type of the attribute is Boolean and the default value is False.

You define compound conditions in the policy rule properties page and not as a separate named condition. See [Configuring Compound Conditions, page 10-41](#).

Custom conditions and Date and Time conditions are called session conditions.

This section contains the following topics:

- [Creating, Duplicating, and Editing a Date and Time Condition, page 9-3](#)
- [Creating, Duplicating, and Editing a Custom Session Condition, page 9-5](#)
- [Deleting a Session Condition, page 9-6](#)
- [Managing Network Conditions, page 9-6](#)

See [ACS 5.x Policy Model, page 3-1](#) for information about additional conditions that you can use in policy rules, although they are not configurable.

Creating, Duplicating, and Editing a Date and Time Condition

Create date and time conditions to specify time intervals and durations. For example, you can define shifts over a specific holiday period. When ACS processes a rule with a date and time condition, the condition is compared to the date and time information of the ACS instance that is processing the request. Clients that are associated with this condition are subject to it for the duration of their session.

The time on the ACS server is used when making policy decisions. Therefore, ensure that you configure date and time conditions that correspond to the time zone in which your ACS server resides. Your time zone may be different from that of the ACS server.

You can duplicate a session condition to create a new session condition that is the same, or similar to, an existing session condition. After duplication is complete, you access each session condition (original and duplicated) separately to edit or delete them.

To create, duplicate, or edit a date and time condition:

-
- Step 1** Choose **Policy Elements > Session Conditions > Date and Time**.
- The Date and Time Conditions page appears.
- Step 2** Do one of the following:
- Click **Create**.
 - Check the check box the condition you want to duplicate and click **Duplicate**.
 - Click the name that you want to modify; or, check the check box the condition that you want to modify and click **Edit**.
- The Date and Time Properties page appears.
- Step 3** Enter valid configuration data in the required fields as described in [Table 9-1](#):

Table 9-1 *Date and Time Properties Page*

Option	Description
General	
Name	Enter a name for the date and time condition.
Description	Enter a description, such as specific days and times of the date and time condition.

Table 9-1 Date and Time Properties Page (continued)

Option	Description
Duration	
Start	<p>Click one of the following options:</p> <ul style="list-style-type: none"> • Start Immediately—Specifies that the rules associated with this condition are valid, starting at the current date. • Start On—Specify a start date by clicking the calendar icon the associated field to choose a specific start date, at which the condition becomes active (at the beginning of the day, indicated by the time 00:00:00 on a 24-hour clock). <p>You can specify time in the <i>hh:mm</i> format.</p>
End	<p>Click one of the following options:</p> <ul style="list-style-type: none"> • No End Date—Specifies that the rules associated with this date and time condition are always active, after the indicated start date. • End By—Specify an end date by clicking the calendar icon the associated field to choose a specific end date, at which the date and time condition becomes inactive (at the end of the day, indicated by the time 23:59:59 on a 24-hour clock) <p>You can specify time in the <i>hh:mm</i> format.</p>
Days and Time	
Days and Time section grid	<p>Each square in the Days and Time grid is equal to one hour. Select a grid square to make the corresponding time active; rules associated with this condition are valid during this time.</p> <p>A green (or darkened) grid square indicates an active hour.</p> <p>Ensure that you configure date and time conditions that correspond to the time zone in which your ACS server resides. Your time zone may be different from that of the ACS server.</p> <p>For example, you may receive an error message if you configure a date and time condition that is an hour ahead of your current time, but that is already in the past with respect to the time zone of your ACS server.</p>
Select All	Click to set all squares in the grid to the active state. Rules associated with this condition are always valid.
Clear All	Click to set all squares in the grid to the inactive state. Rules associated with this condition are always invalid.
Undo All	Click to remove your latest changes for the active and inactive day and time selections for the date and time group.

To add date and time conditions to a policy, you must first customize the rule table. See [Customizing a Policy, page 10-4](#).

Step 4 Click **Submit**.

The date and time condition is saved. The Date and Time Conditions page appears with the new date and time condition that you created or duplicated.



Note

ACS has services and resources that are time sensitive. So, it is advised to restart all services after performing operations such as changing the clock, time zone, or NTP. If you do not restart after these operations, there are possibilities that it may break the functionalities such as AD, database connections, and cryptographic materials.

Related Topics

- [Creating, Duplicating, and Editing a Custom Session Condition, page 9-5](#)
- [Deleting a Session Condition, page 9-6](#)
- [Configuring Access Service Policies, page 10-23](#)

Creating, Duplicating, and Editing a Custom Session Condition

The protocol and identity dictionaries contain a large number of attributes. To use any of these attributes as a condition in a policy rule, you must first create a custom condition for the attribute. In this way, you define a smaller subset of attributes to use in policy conditions, and present a smaller focused list from which to choose condition types for rule tables.

You can also include protocol and identity attributes within compound conditions. See [Configuring Compound Conditions, page 10-41](#) for more information on compound conditions.

To create a custom condition, you must select a specific protocol (RADIUS or TACACS+) or identity attribute from one of the dictionaries, and name the custom condition. See [Configuring Global System Options, page 18-1](#) for more information on protocol and identity dictionaries.

When you create a custom condition that includes identity or RADIUS attributes, you can also include the definition of the attributes. You can thus easily view any existing custom conditions associated with a particular attribute.

To create, duplicate, or edit a custom session condition:

Step 1 Choose **Policy Elements > Session Conditions > Custom**.

The Custom Conditions page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box the condition you want to duplicate and click **Duplicate**.
- Click the name that you want to modify; or, check the check box the condition that you want to modify and click **Edit**.

The Custom Condition Properties page appears.

Step 3 Enter valid configuration data in the required fields as shown in [Table 9-2](#):

Table 9-2 *Policy Custom Condition Properties Page*

Option	Description
General	
Name	Name of the custom condition.
Description	Description of the custom condition.
Condition	
Dictionary	Choose a specific protocol or identity dictionary from the drop-down list box.
Attribute	Click Select to display the list of external identity store dictionaries based on the selection you made in the Dictionary field. Select the attribute that you want to associate with the custom condition, then click OK . If you are editing a custom condition that is in use in a policy, you cannot edit the attribute that it references.

To add custom conditions to a policy, you must first customize the rule table. See [Customizing a Policy, page 10-4](#).

Step 4 Click **Submit**.

The new custom session condition is saved. The Custom Condition page appears with the new custom session condition. Clients that are associated with this condition are subject to it for the duration of their session.

Related Topics

- [Creating, Duplicating, and Editing a Date and Time Condition, page 9-3](#)
- [Deleting a Session Condition, page 9-6](#)
- [Configuring Access Service Policies, page 10-23](#)

Deleting a Session Condition

To delete a session condition:

Step 1 Choose **Policy Elements > Session Conditions > *session condition***, where *session condition* is Date and Time or Custom.

The Session Condition page appears.

Step 2 Check one or more check boxes the session conditions that you want to delete and click **Delete**.

The following message appears:

Are you sure you want to delete the selected item/items?

Step 3 Click **OK**.

The Session Condition page appears without the deleted custom session conditions.

Related Topics

- [Creating, Duplicating, and Editing a Date and Time Condition, page 9-3](#)
- [Creating, Duplicating, and Editing a Custom Session Condition, page 9-5](#)

Managing Network Conditions

Filters are reusable network conditions that you create for end stations, network devices, and network device ports. Filters enable ACS 5.8.1 to do the following:

- Decide whether or not to grant network access to users and devices.
- Decide on the identity store, service, and so on to be used in policies.

After you create a filter with a name, you can reuse this filter multiple times across various rules and policies by referring to its name.

**Note**

The filters in ACS 5.8.1 are similar to the NARs in ACS 4.x. In ACS 4.x, the NARs were based on either the user or user group. In 5.8.1, the filters are independent conditions that you can reuse across various rules and policies.

ACS offers three types of filters:

- **End Station Filter**—Filters end stations, such as a laptop or printer that initiates a connection based on the end station's IP address, MAC address, CLID number, or DNIS number.

The end station identifier can be the IP address, MAC address, or any other string that uniquely identifies the end station. It is a protocol-agnostic attribute of type string that contains a copy of the end station identifier:

- In a RADIUS request, this identifier is available in Attribute 31 (Calling-Station-Id).
- In a TACACS request, ACS obtains this identifier from the remote address field of the start request (of every phase). It takes the remote address value before the slash (/) separator, if it is present; otherwise, it takes the entire remote address value.

The end station IP address is either an IPv4 or IPv6 of the end station identifier. The end station MAC is a normalized MAC address of the end station identifier.

- **Device Filter**—Filters a network device (AAA client) that acts as a Policy Enforcement Point (PEP) to the end station based on the network device's IP address or name, or the network device group that it belongs to.

The device identifier can be the IP address or name of the device, or it can be based on the network device group to which the device belongs.

The IP address is a protocol-agnostic attribute of type IPv4 or IPv6, which contains a copy of the device IP address that is obtained from the request:

- In a RADIUS request, if Attribute 4 (NAS-IP-Address) is present, ACS obtains the IP address from Attribute 4; otherwise, if Attribute 32 (NAS-Identifier) is present, ACS obtains the IP address from Attribute 32, or it obtains the IP address from the packet that it receives.
- In a TACACS request, the IP address is obtained from the packet that ACS receives.

The device name is an attribute of type string that contains a copy of the device name derived from the ACS repository.

The device dictionary (the NDG dictionary) contains network device group attributes such as Location, Device Type, or other dynamically created attributes that represent NDGs. These attributes, in turn, contain the groups that the current device is related to.

- **Device Port Filter**—Filters the physical port of the device that the end station is connected to. Filtering is based on the device's IP address, name, NDG it belongs to, and port.

The device port identifier is an attribute of type string:

- In a RADIUS request, if Attribute 5 (NAS-Port) is present in the request, ACS obtains the value from Attribute 5; or, if Attribute 87 (NAS-Port-Id) is present in the request, ACS obtains the request from Attribute 87.
- In a TACACS request, ACS obtains this identifier from the port field of the start request (of every phase).

The device name is an attribute of type string that contains a copy of the device name derived from the ACS repository.

The device dictionary (the NDG dictionary) contains network device group attributes such as Location, Device Type, or other dynamically created attributes that represent NDGs. These attributes, in turn, contain the groups that the current device is related to.

You can create, duplicate, and edit these filters. You can also do a bulk import of the contents within a filter from a .csv file and export the filters from ACS to a .csv file. See [Importing Network Conditions, page 9-8](#) for more information on how to do a bulk import of network conditions.

This section contains the following topics:

- [Importing Network Conditions, page 9-8](#)
- [Exporting Network Conditions, page 9-9](#)
- [Creating, Duplicating, and Editing End Station Filters, page 9-9](#)
- [Creating, Duplicating, and Editing Device Filters, page 9-12](#)
- [Creating, Duplicating, and Editing Device Port Filters, page 9-14](#)

Importing Network Conditions

You can use the bulk import function to import the contents from the following network conditions:

- End station filters
- Device filters
- Device port filters

For bulk import, you must download the .csv file template from ACS, add the records that you want to import to the .csv file, and save it to your hard drive. Use the Download Template function to ensure that your .csv file adheres to the requirements.

The .csv templates for end station filters, device filters, and device port filters are specific to their type; for example, you cannot use a downloaded template accessed from the End Station Filters page to import device filters or device port filters. Within the .csv file, you must adhere to these requirements:

- Do not alter the contents of the first record (the first line, or row, of the .csv file).
- Use only one line for each record.
- Do not imbed new-line characters in any fields.
- For non-English languages, encode the .csv file in utf-8 encoding, or save it with a font that supports Unicode.

The import process does not add filters to the existing list of filters in ACS, but instead replaces the existing list. When you import records from a .csv file, it replaces the existing filter configuration in ACS and replaces it with the filter configuration from the .csv file.

Step 1 Click the **Replace from File** button on the End Station Filter, Device Filter, or Device Port Filter page of the web interface.

The Replace from File dialog box appears.

Step 2 Click **Download Template** to download the .csv file template if you do not have it.

Step 3 Click **Browse** to navigate to your .csv file.

Step 4 Click **Start Replace** to start the bulk import process.

The import progress is shown on the same page. You can monitor the bulk import progress. Data transfer failures of any records within your .csv file are displayed.

Step 5 Click **Close** to close the Import Progress window.

You can submit only one .csv file to the system at one time. If an import is under way, an additional import cannot succeed until the original import is complete.



Note

Instead of downloading the template and creating an import file, you can use the export file of the particular filter, update the information in that file, save it, and reuse it as your import file.

Exporting Network Conditions

ACS 5.8.1 offers you a bulk export function to export the filter configuration data in the form of a .csv file. You can export the following filter configurations:

- End Station Filters
- Device Filters
- Device Port Filters

From the create, edit, or duplicate page of any of the filters, click **Export to File** to save the filter configuration as a .csv file on your local hard drive.

Creating, Duplicating, and Editing End Station Filters

Use the End Station Filters page to create, duplicate, and edit end station filters. To do this:

Step 1 Choose **Policy Elements > Session Conditions > Network Conditions > End Station Filters**.

The End Station Filters page appears with a list of end station filters that you have configured.

Step 2 Click **Create**. You can also:

- Check the check box the end station filter that you want to duplicate, then click **Duplicate**.
- Check the check box the end station filter that you want to edit, then click **Edit**.
- Click **Export** to save a list of end station filters in a .csv file. For more information, see [Exporting Network Conditions, page 9-9](#).
- Click **Replace from File** to perform a bulk import of end station filters from a .csv import file. For more information, see [Importing Network Conditions, page 9-8](#).

Step 3 Enter the values for the following fields:

- Name—Name of the end station filter.
- Description—A description of the end station filter.

Step 4 Edit the fields in one or more of the following tabs:

- IP Address—See [Defining IP Address-Based End Station Filters, page 9-10](#) for a description of the fields in this tab.
- MAC Address—See [Defining MAC Address-Based End Station Filters, page 9-11](#) for a description of the fields in this tab.
- CLI/DNIS—See [Defining CLI or DNIS-Based End Station Filters, page 9-11](#) for a description of the fields in this tab.



Note To configure a filter, at a minimum, you must enter filter criteria in at least one of the three tabs.

Step 5 Click **Submit** to save the changes.

Related Topics

- [Managing Network Conditions, page 9-6](#)
- [Importing Network Conditions, page 9-8](#)
- [Creating, Duplicating, and Editing Device Filters, page 9-12](#)
- [Creating, Duplicating, and Editing Device Port Filters, page 9-14](#)

Defining IP Address-Based End Station Filters

You can create, duplicate, and edit the IP addresses of end stations that you want to permit or deny access to. To do this:

Step 1 From the IP Address tab, do one of the following:

- Click **Create**.
- Check the check box the IP-based end station filter that you want to duplicate, then click **Duplicate**.
- Check the check box the IP-based end station filter that you want to edit, then click **Edit**.
- A dialog box appears.

Step 2 Choose either of the following:

- **Single IP Address**—If you choose this option, you must enter a valid address, as follows:
 - IPv4 address in the format *x.x.x.x*, where *x* can be any number from 0 to 255.
 - IPv6 address in the format *x:x:x:x:x:x:x:x*, where *x* represents one to four hexadecimal digits of the eight 16-bit pieces of the address. This can be either numbers from 0 to 9 or letters from A to F.
- **IP Range(s)**—If you choose this option, you must enter a valid IPv4 address and subnet mask to filter a range of IP addresses. By default, the subnet mask value for IPv4 is 32, and the IPv6 value is 128.



Note IPv6 ranges are not supported in ACS 5.8.1.



Note IPv6 addresses are supported only in TACACS+ protocols.

Step 3 Click **OK**.

Related Topics

- [Managing Network Conditions, page 9-6](#)
- [Creating, Duplicating, and Editing End Station Filters, page 9-9](#)
- [Defining MAC Address-Based End Station Filters, page 9-11](#)

- [Defining CLI or DNIS-Based End Station Filters, page 9-11](#)

Defining MAC Address-Based End Station Filters

You can create, duplicate, and edit the MAC addresses of end stations or destinations that you want to permit or deny access to. To do this:

-
- Step 1** From the MAC Address tab, do one of the following:
- Click **Create**.
 - Check the check box the MAC address-based end station filter that you want to duplicate, then click **Duplicate**.
 - Check the check box the MAC address-based end station filter that you want to edit, then click **Edit**.
 - A dialog box appears.
- Step 2** Check the **End Station MAC** check box to enter the MAC address of the end station.
You can optionally set this field to ANY to refer to any MAC address.
- Step 3** Check the **Destination MAC** check box to enter the MAC address of the destination machine.
You can optionally set this field to ANY to refer to any MAC address.



Note

You must enter the MAC address in one of the following formats: `xxxxxxxxxxxx`, `xx-xx-xx-xx-xx-xx`, `xx:xx:xx:xx:xx:xx`, or `xxxx.xxxx.xxxx`, where x can be any number from 0 to 9 or A through F. You cannot use wildcard characters for MAC address.

- Step 4** Click **OK**.
-

Related Topics

- [Managing Network Conditions, page 9-6](#)
- [Creating, Duplicating, and Editing End Station Filters, page 9-9](#)
- [Defining IP Address-Based End Station Filters, page 9-10](#)
- [Defining CLI or DNIS-Based End Station Filters, page 9-11](#)

Defining CLI or DNIS-Based End Station Filters

You can create, duplicate, and edit the CLI and DNIS number of the end stations or destinations that you want to permit or deny access to. To do this:

-
- Step 1** From the CLI/DNIS tab, do one of the following:
- Click **Create**.
 - Check the check box the CLI or DNIS-based end station filter that you want to duplicate, then click **Duplicate**.
 - Check the check box the CLI or DNIS-based end station filter that you want to edit, then click **Edit**.
 - A dialog box appears.
- Step 2** Check the **CLI** check box to enter the CLI number of the end station.
You can optionally set this field to ANY to refer to any CLI number.

- Step 3** Check the **DNIS** check box to enter the DNIS number of the destination machine.
You can optionally set this field to ANY to refer to any DNIS number.



Note You can use ? and * wildcard characters to refer to any single character or a series of one or more successive characters respectively.

- Step 4** Click **OK**.

Related Topics

- [Managing Network Conditions, page 9-6](#)
- [Creating, Duplicating, and Editing End Station Filters, page 9-9](#)
- [Defining IP Address-Based End Station Filters, page 9-10](#)
- [Defining MAC Address-Based End Station Filters, page 9-11](#)

Creating, Duplicating, and Editing Device Filters

Use the Device Filters page to create, duplicate, and edit device filters. To do this:

- Step 1** Choose **Policy Elements > Session Conditions > Network Conditions > Device Filters**.
The Device Filters page appears with a list of device filters that you have configured.
- Step 2** Click **Create**. You can also:
- Check the check box the device filter that you want to duplicate, then click **Duplicate**.
 - Check the check box the device filter that you want to edit, then click **Edit**.
 - Click **Export** to save a list of device filters in a .csv file. For more information, see [Exporting Network Conditions, page 9-9](#).
 - Click **Replace from File** to perform a bulk import of device filters from a .csv import file. For more information, see [Importing Network Conditions, page 9-8](#).
- Step 3** Enter the values for the following fields:
- Name—Name of the device filter.
 - Description—A description of the device filter.
- Step 4** Edit the fields in any or all of the following tabs:
- IP Address—See [Defining IP Address-Based Device Filters, page 9-13](#) for a description of the fields in this tab.
 - Device Name—See [Defining Name-Based Device Filters, page 9-13](#) for a description of the fields in this tab.
 - Network Device Group—See [Defining NDG-Based Device Filters, page 9-14](#) for a description of the fields in this tab.



Note To configure a filter, at a minimum, you must enter filter criteria in at least one of the three tabs.

Step 5 Click **Submit** to save the changes.

Related Topics

- [Managing Network Conditions, page 9-6](#)
- [Importing Network Conditions, page 9-8](#)
- [Creating, Duplicating, and Editing End Station Filters, page 9-9](#)
- [Creating, Duplicating, and Editing Device Port Filters, page 9-14](#)

Defining IP Address-Based Device Filters

You can create, duplicate, and edit the IP addresses of network devices that you want to permit or deny access to. To do this:

Step 1 From the IP Address tab, do one of the following:

- Click **Create**.
- Check the check box the IP-based device filter that you want to duplicate, then click **Duplicate**.
- Check the check box the IP-based device filter that you want to edit, then click **Edit**.

A dialog box appears.

Step 2 Choose either of the following:

- **Single IP Address**—If you choose this option, you must enter a valid address, as follows:
 - IPv4 address in the format *x.x.x.x*, where *x* can be any number from 0 to 255.
 - IPv6 address in the format *x:x:x:x:x:x:x:x*, where *x* represents one to four hexadecimal digits of the eight 16-bit pieces of the address. This can be either numbers from 0 to 9 or letters from A to F.
- **IP Range(s)**—If you choose this option, you must enter a valid IPv4 or IPv6 address and subnet mask to filter a range of IP addresses. By default, the subnet mask value for IPv4 is 32, and the IPv6 value is 128.



Note

IPv6 ranges are not supported in ACS 5.8.1.

Step 3 Click **OK**.

Related Topics

- [Managing Network Conditions, page 9-6](#)
- [Creating, Duplicating, and Editing Device Filters, page 9-12](#)
- [Defining Name-Based Device Filters, page 9-13](#)
- [Defining NDG-Based Device Filters, page 9-14](#)

Defining Name-Based Device Filters

You can create, duplicate, and edit the name of the network device that you want to permit or deny access to. To do this:

-
- Step 1** From the Device Name tab, do one of the following:
- Click **Create**.
 - Check the check box the name-based device filter that you want to duplicate, then click **Duplicate**.
 - Check the check box the name-based device filter that you want to edit, then click **Edit**.
- A dialog box appears.
- Step 2** Click **Select** to choose the network device that you want to filter.
- Step 3** Click **OK**.
-

Related Topics

- [Managing Network Conditions, page 9-6](#)
- [Creating, Duplicating, and Editing Device Filters, page 9-12](#)
- [Defining IP Address-Based Device Filters, page 9-13](#)
- [Defining NDG-Based Device Filters, page 9-14](#)

Defining NDG-Based Device Filters

You can create, duplicate, and edit the name of the network device group type that you want to permit or deny access to. To do this:

-
- Step 1** From the Network Device Group tab, do one of the following:
- Click **Create**.
 - Check the check box the NDG-based device filter that you want to duplicate, then click **Duplicate**.
 - Check the check box the NDG-based device filter that you want to edit, then click **Edit**.
- A dialog box appears.
- Step 2** Click **Select** to choose the network device group type that you want to filter.
- Step 3** Click **Select** to choose the network device group value that you want to filter.
- Step 4** Click **OK**.
-

Related Topics

- [Managing Network Conditions, page 9-6](#)
- [Creating, Duplicating, and Editing Device Filters, page 9-12](#)
- [Defining IP Address-Based Device Filters, page 9-13](#)
- [Defining Name-Based Device Filters, page 9-13](#)

Creating, Duplicating, and Editing Device Port Filters

Use the Device Port Filters page to create, duplicate, and edit device port filters. To do this:

-
- Step 1** Choose **Policy Elements > Session Conditions > Network Conditions > Device Port Filters**.
-

The Device Port Filters page appears with a list of device port filters that you have configured.

Step 2 Click **Create**. You can also:

- Check the check box the device port filter that you want to duplicate, then click **Duplicate**.
- Check the check box the device port filter that you want to edit, then click **Edit**.
- Click **Export** to save a list of device port filters in a .csv file. For more information, see [Exporting Network Conditions, page 9-9](#).
- Click **Replace from File** to perform a bulk import of device port filters from a .csv import file. For more information, see [Importing Network Conditions, page 9-8](#).

Step 3 Enter the values for the following fields:

- Name—Name of the device port filter.
- Description—A description of the device port filter.

Step 4 Edit the fields in any or all of the following tabs:

- IP Address—See [Defining IP Address-Based Device Port Filters, page 9-15](#) for a description of the fields in this tab.
- Device Name—See [Defining NDG-Based Device Port Filters, page 9-17](#) for a description of the fields in this tab.
- Network Device Group—See [Defining NDG-Based Device Port Filters, page 9-17](#) for a description of the fields in this tab.



Note

To configure a filter, at a minimum, you must enter filter criteria in at least one of the three tabs.

Step 5 Click **Submit** to save the changes.

Related Topics

- [Managing Network Conditions, page 9-6](#)
- [Importing Network Conditions, page 9-8](#)
- [Creating, Duplicating, and Editing End Station Filters, page 9-9](#)
- [Creating, Duplicating, and Editing Device Filters, page 9-12](#)

Defining IP Address-Based Device Port Filters

You can create, duplicate, and edit the IP addresses of the network device ports that you want to permit or deny access to. To do this:

Step 1 From the IP Address tab, do one of the following:

- Click **Create**.
- Check the check box the IP-based device port filter that you want to duplicate, then click **Duplicate**.
- Check the check box the IP-based device port filter that you want to edit, then click **Edit**.

A dialog box appears.

Step 2 Choose either of the following:

- Single IP Address—If you choose this option, you must enter a valid address, as follows:

- IPv4 address in the format *x.x.x.x*, where *x* can be any number from 0 to 255.
- IPv6 address in the format *x:x:x:x:x:x:x:x*, where *x* represents one to four hexadecimal digits of the eight 16-bit pieces of the address. This can be either numbers from 0 to 9 or letters from A to F.
- IP Range(s)—If you choose this option, you must enter a valid IPv4 or IPv6 address and subnet mask to filter a range of IP addresses. By default, the subnet mask value for IPv4 is 32, and the IPv6 value is 128.



Note IPv6 ranges are not supported in ACS 5.8.1.

Step 3 Check the **Port** check box and enter the port number. This field is of type string and can contain numbers or characters. You can use the following wildcard characters:

- ?—match a single character
- *—match a set of characters

For example, the string “p*1*” would match any word that starts with the letter “p” and contains the number 1, such as port1, port15, and so on.

Step 4 Click **OK**.

Related Topics

- [Managing Network Conditions, page 9-6](#)
- [Creating, Duplicating, and Editing Device Port Filters, page 9-14](#)
- [Defining Name-Based Device Port Filters, page 9-16](#)
- [Defining NDG-Based Device Port Filters, page 9-17](#)

Defining Name-Based Device Port Filters

You can create, duplicate, and edit the name of the network device and the port to which you want to permit or deny access. To do this:

Step 1 From the Device Name tab, do one of the following:

- Click **Create**.
- Check the check box the name-based device port filter that you want to duplicate, then click **Duplicate**.
- Check the check box the name-based device port filter that you want to edit, then click **Edit**.
- A dialog box appears.

Step 2 Click **Select** to choose the network device that you want to filter.

Step 3 Check the **Port** check box and enter the port number.

Step 4 Click **OK**.

Related Topics

- [Managing Network Conditions, page 9-6](#)

- [Creating, Duplicating, and Editing Device Port Filters, page 9-14](#)
- [Defining IP Address-Based Device Port Filters, page 9-15](#)
- [Defining NDG-Based Device Port Filters, page 9-17](#)

Defining NDG-Based Device Port Filters

You can create, duplicate, and edit the network device group type and the port to which you want to permit or deny access. To do this:

-
- Step 1** From the Network Device Group tab, do one of the following:
- Click **Create**.
 - Check the check box the NDG-based device port filter that you want to duplicate, then click **Duplicate**.
 - Check the check box the NDG-based device port filter that you want to edit, then click **Edit**.
- A dialog box appears.
- Step 2** Click **Select** to choose the network device group type that you want to filter.
- Step 3** Click **Select** to choose the network device group value that you want to filter.
- Step 4** Check the **Port** check box and enter the port number.
- Step 5** Click **OK**.
-

Related Topics

- [Managing Network Conditions, page 9-6](#)
- [Creating, Duplicating, and Editing Device Filters, page 9-12](#)
- [Defining IP Address-Based Device Filters, page 9-13](#)
- [Defining Name-Based Device Filters, page 9-13](#)

Managing Authorizations and Permissions

You define authorizations and permissions to determine the results associated with a specific policy rule.

You can define:

- Authorization profiles for network access authorization (for RADIUS).
- Shell profiles for TACACS+ shell sessions and command sets for device administration.
- Downloadable ACLs.
- Security groups and security group ACLs for Cisco Security Group Access. See [ACS and Cisco Security Group Access, page 4-22](#), for information on configuring these policy elements.

These topics describe how to manage authorizations and permissions:

- [Creating, Duplicating, and Editing Authorization Profiles for Network Access, page 9-18](#)
- [Creating and Editing Security Groups, page 9-22](#)
- [Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-23](#)
- [Creating, Duplicating, and Editing Command Sets for Device Administration, page 9-28](#)

- [Creating, Duplicating, and Editing Downloadable ACLs, page 9-31](#)
- [Deleting an Authorizations and Permissions Policy Element, page 9-32](#)
- [Configuring Security Group Access Control Lists, page 9-32](#)

Creating, Duplicating, and Editing Authorization Profiles for Network Access

You create authorization profiles to define how different types of users are authorized to access the network. For example, you can define that a user attempting to access the network over a VPN connection is treated more strictly than a user attempting to access the network through a wired connection.

An authorization profile defines the set of attributes and values that the Access-Accept response returns. You can specify:

- Common data, such as VLAN information, URL for redirect, and more. This information is automatically converted to the raw RADIUS parameter information.
- RADIUS authorization parameters—You can select any RADIUS attribute and specify the corresponding value to return.

You can duplicate an authorization profile to create a new authorization profile that is the same, or similar to, an existing authorization profile. After duplication is complete, you access each authorization profile (original and duplicated) separately to edit or delete them.

After you create authorization profiles, you can use them as results in network access session authorization policies.

To create, duplicate, or edit an authorization profile:

- Step 1** Choose **Policy Elements > Authorization and Permissions > Network Access > Authorization Profile**.

The Authorization Profiles page appears with the fields described in [Table 9-3](#):

Table 9-3 *Authorization Profiles Page*

Option	Description
Name	List of existing network access authorization definitions.
Description	<i>Display only.</i> The description of the network access authorization definition.

- Step 2** Do one of the following:
- Click **Create**.
 - Check the check box the authorization profile that you want to duplicate and click **Duplicate**.
 - Click the name that you want to modify; or, check the check box the name that you want to modify and click **Edit**.

The Authorization Profile Properties page appears.

- Step 3** Enter valid configuration data in the required fields in each tab. See:
- [Specifying Authorization Profiles, page 9-19](#)
 - [Specifying Common Attributes in Authorization Profiles, page 9-19](#)

- [Specifying RADIUS Attributes in Authorization Profiles, page 9-20](#)

Step 4 Click **Submit**.

The authorization profile is saved. The Authorization Profiles page appears with the authorization profile that you created or duplicated.

Specifying Authorization Profiles

Use this tab to configure the name and description for a network access authorization profile.

Step 1 Choose **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, then click:

- **Create** to create a new network access authorization definition.
- **Duplicate** to duplicate a network access authorization definition.
- **Edit** to edit a network access authorization definition.

Step 2 Complete the required fields of the Authorization Profile: General page as shown in [Table 9-4](#):

Table 9-4 Authorization Profile: General Page

Option	Description
Name	The name of the network access authorization definition.
Description	The description of the network access authorization definition.

Step 3 Click one of the following:

- **Submit** to save your changes and return to the Authorization Profiles page.
- The **Common Tasks** tab to configure common tasks for the authorization profile; see [Specifying Common Attributes in Authorization Profiles, page 9-19](#).
- The **RADIUS Attributes** tab to configure RADIUS attributes for the authorization profile; see [Specifying RADIUS Attributes in Authorization Profiles, page 9-20](#).

Specifying Common Attributes in Authorization Profiles

Use this tab to specify common RADIUS attributes to include in a network access authorization profile. ACS converts the specified values to the required RADIUS attribute-value pairs and displays them in the RADIUS attributes tab.

Step 1 Choose **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, then click:

- **Create** to create a new network access authorization definition, then click the **Common Tasks** tab.
- **Duplicate** to duplicate a network access authorization definition, then click the **Common Tasks** tab.
- **Edit** to edit a network access authorization definition, then click the **Common Tasks** tab.

Step 2 Complete the required fields of the Authorization Profile: Common Tasks page as shown in [Table 9-5](#):

Table 9-5 Authorization Profile: Common Tasks Page

Option	Description
ACLS	
Downloadable ACL Name	Includes a defined downloadable ACL. See Creating, Duplicating, and Editing Downloadable ACLs, page 9-31 for information about defining a downloadable ACL.
Filter-ID ACL	Includes an ACL Filter ID.
Proxy ACL	Includes a proxy ACL.
Voice VLAN	
Permission to Join	Select Static . A value for this parameter is displayed.
VLAN	
VLAN ID/Name	Includes a VLAN assignment.
Reauthentication	
Reauthentication Timer	Select whether to use a session timeout value. <ul style="list-style-type: none"> If you select Static, you must enter a value in the Seconds field. The default value is 3600 seconds. If you select Dynamic, you must select the dynamic parameters.
Maintain Connectivity during Reauthentication	Click Yes to ensure connectivity is maintained while reauthentication is performed. By default, Yes is selected. This field is enabled only if you define the Reauthentication Timer.
QoS	
Input Policy Map	Includes a QoS input policy map.
Output Policy Map	Includes a QoS output policy map.
802.1X-REV	
LinkSec Security Policy	If you select Static , you must select a value for the 802.1X-REV LinkSec security policy. Valid options are: <ul style="list-style-type: none"> must-not-secure should-secure must-secure
URL Redirect	
When a URL is defined for Redirect an ACL must also be defined	
URL for Redirect	Includes a URL redirect.
URL Redirect ACL	Includes the name of the access control list (ACL) for URL redirection. When you define a URL redirect, you must also define an ACL for the URL redirection.

Specifying RADIUS Attributes in Authorization Profiles

Use this tab to configure which RADIUS attributes to include in the Access-Accept packet for an authorization profile. This tab also displays the RADIUS attribute parameters that you choose in the Common Tasks tab.

- Step 1** Choose **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**, then click:
- **Create** to create a new network access authorization definition, then click the **RADIUS Attributes** tab.
 - Check the check box the authentication profile that you want to duplicate, click **Duplicate**, and then click the **RADIUS Attributes** tab.
 - Check the check box the authentication profile that you want to duplicate, click **Edit**, and then click the **RADIUS Attributes** tab.
- Step 2** Complete the required fields of the Authorization Profile: RADIUS Attributes page as shown in [Table 9-6](#):

Table 9-6 *Authorization Profile: RADIUS Attributes Page*

Option	Description
Common Tasks Attributes	Displays the names, values, and types for the attributes that you defined in the Common Tasks tab.
Manually Entered	Use this section to define RADIUS attributes to include in the authorization profile. As you define each attribute, its name, value, and type appear in the table. To: <ul style="list-style-type: none"> • Add a RADIUS attribute, fill in the fields below the table and click Add. • Edit a RADIUS attribute, select the appropriate row in the table and click Edit. The RADIUS parameters appear in the fields below the table. Edit as required, then click Replace.
Dictionary Type	Choose the dictionary that contains the RADIUS attribute you want to use.
RADIUS Attribute	<p>Name of the RADIUS attribute. Click Select to choose a RADIUS attribute from the specified dictionary.</p> <p>You must manually add VPN attributes to the authorization profile to authenticate VPN devices in your network. ACS can work with different Layer 2 and Layer 3 protocols, such as:</p> <ul style="list-style-type: none"> • IPSec—Operates at Layer 3; no mandatory attributes need to be configured in the ACS authorization profile, but you can configure optional attributes. • L2TP—For L2TP tunneling, you must configure ACS with: <ul style="list-style-type: none"> – CVPN3000/ASA/PIX7.x-Tunneling Protocols—This attribute specifies the type of tunneling to be used. – CVPN3000/ASA/PIX7.x-L2TP-Encryption—This attribute, when set, enables VPN3000 to communicate to the client the type of Microsoft Point-to-Point Encryption (MPPE) key that must be used, either the MSCHAPv1 or MSCHAPv2 authentication method. • PPTP—For PPTP tunneling, you must configure ACS with: <ul style="list-style-type: none"> – CVPN3000/ASA/PIX7.x-Tunneling Protocols—This attribute specifies the type of tunneling to be used. – CVPN3000/ASA/PIX7.x-PPTP-Encryption—This attribute, when set, enables VPN3000 to communicate to the client the type of Microsoft Point-to-Point Encryption (MPPE) key that must be used, either the MSCHAPv1 or MSCHAPv2 authentication method.

Table 9-6 Authorization Profile: RADIUS Attributes Page (continued)

Option	Description
Attribute Type	Client vendor type of the attribute, from which ACS allows access requests. For a description of the attribute types, refer to Cisco IOS documentation for the release of Cisco IOS software that is running on your AAA clients.
Attribute Value	<p>Value of the attribute. Click Select for a list of attribute values. For a description of the attribute values, refer to Cisco IOS documentation for the release of Cisco IOS software that is running on your AAA clients.</p> <p>For tunneled protocols, ACS provides for attribute values with specific tags to the device within the access response according to RFC 2868.</p> <p>If you choose Tagged Enum or Tagged String as the RADIUS Attribute type, the Tag field appears. For the tag value, enter a number that ACS will use to group attributes belonging to the same tunnel.</p> <p>For the Tagged Enum attribute type:</p> <ul style="list-style-type: none"> Choose an appropriate attribute value. Enter an appropriate tag value (0–31). <p>For the Tagged String attribute type:</p> <ul style="list-style-type: none"> Enter an appropriate string attribute value (up to 256 characters). Enter an appropriate tag value (0–31).

Step 3 To configure:

- Basic information of an authorization profile; see [Specifying Authorization Profiles, page 9-19](#).
- Common tasks for an authorization profile; see [Specifying Common Attributes in Authorization Profiles, page 9-19](#).

Creating and Editing Security Groups

Use this page to view names and details of security groups and security group tags (SGTs), and to open pages to create, duplicate, and edit security groups.

When you create a security group, ACS generates a unique SGT. Network devices can query ACS for SGT information. The network device uses the SGT to tag, or paint, packets at ingress, so that the packets can be filtered at Egress according to the Egress policy. See [Egress Policy Matrix Page, page 10-47](#), for information on configuring an Egress policy.

Step 1 Choose **Policy Elements > Authorizations and Permissions > Network Access > Security Groups**.

The Security Groups page appears as described in [Table 9-7](#):

Table 9-7 Security Groups Page

Option	Description
Name	The name of the security group.

Table 9-7 Security Groups Page

Option	Description
SGT (Dec / Hex)	Representation of the security group tag in decimal and hexadecimal format.
Description	The description of the security group.

Step 2 Click:

- **Create** to create a new security group.
- **Duplicate** to duplicate a security group.
- **Edit** to edit a security group.

Step 3 Enter the required information in the Name and Description fields, then click **Submit**.**Related Topic**

- [Creating Security Groups, page 4-23](#)

Creating, Duplicating, and Editing a Shell Profile for Device Administration

You can configure Cisco IOS shell profile and command set authorization. Shell profiles and command sets are combined for authorization purposes. Shell profile authorization provides decisions for the following capabilities for the user requesting authorization and is enforced for the duration of a user's session:

- Privilege level.
- General capabilities, such as device administration and network access.

Shell profile definitions are split into two components:

- Common tasks
- Custom attributes

The Common Tasks tab allows you to select and configure the frequently used attributes for the profile. The attributes that are included here are those defined by the TACACS protocol draft specification that are specifically relevant to the shell service. However, the values can be used in the authorization of requests from other services.

The Custom Attributes tab allows you to configure additional attributes. Each definition consists of the attribute name, an indication of whether the attribute is mandatory or optional, and the value for the attribute. Custom attributes can be defined for nonshell services.

For a description of the attributes that you specify in shell profiles, see Cisco IOS documentation for the specific release of Cisco IOS software that is running on your AAA clients.

After you create shell profiles and command sets, you can use them in authorization and permissions within rule tables.

You can duplicate a shell profile if you want to create a new shell profile that is the same, or similar to, an existing shell profile.

After duplication is complete, you access each shell profile (original and duplicated) separately to edit or delete them.

To create, duplicate, or edit a shell profile:

-
- Step 1** Choose **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**. The Shell Profiles page appears.
- Step 2** Do one of the following:
- Click **Create**.
 - Check the check box the shell profile that you want to duplicate and click **Duplicate**.
 - Click the name that you want to modify; or, check the check box the name that you want to modify and click **Edit**.
- The Shell Profile Properties page General tab appears.
- Step 3** Enter valid configuration data in the required fields in each tab. As a minimum configuration, you must enter a unique name for the shell profile; all other fields are optional. See:
- [Defining General Shell Profile Properties, page 9-24](#)
 - [Defining Common Tasks, page 9-25](#)
 - [Defining Custom Attributes, page 9-27](#)
- Step 4** Click **Submit**.
- The shell profile is saved. The Shell Profiles page appears with the shell profile that you created or duplicated.
-

Related Topics

- [Creating, Duplicating, and Editing Authorization Profiles for Network Access, page 9-18](#)
- [Creating, Duplicating, and Editing Command Sets for Device Administration, page 9-28](#)
- [Deleting an Authorizations and Permissions Policy Element, page 9-32](#)
- [Configuring Shell/Command Authorization Policies for Device Administration, page 10-36](#)

Defining General Shell Profile Properties

Use this page to define a shell profile's general properties.

-
- Step 1** Choose **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**, then do one of the following:
- Click **Create**.
 - Check the check box the shell profile that you want to duplicate and click **Duplicate**.
 - Click the name that you want to modify; or, check the check box the name that you want to modify and click **Edit**.
- Step 2** Complete the Shell Profile: General fields as described in [Table 9-8](#):

Table 9-8 *Shell Profile: General Page*

Option	Description
Name	The name of the shell profile.
Description	(Optional) The description of the shell profile.

Step 3 Click:

- **Submit** to save your changes and return to the Shell Profiles page.
- The **Common Tasks** tab to configure privilege levels for the authorization profile; see [Defining Common Tasks, page 9-25](#).
- The **Custom Attributes** tab to configure RADIUS attributes for the authorization profile; see [Defining Custom Attributes, page 9-27](#).

Related Topics

- [Defining Common Tasks, page 9-25](#)
- [Defining Custom Attributes, page 9-27](#)

Defining Common Tasks

Use this page to define a shell profile's privilege level and attributes. The attributes are defined by the TACACS+ protocol.

For a description of the attributes, refer to Cisco IOS documentation for the release of Cisco IOS software that is running on your AAA clients.

- Step 1** Choose **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**, then click:
- **Create** to create a new shell profile, then click **Common Tasks**.
 - **Duplicate** to duplicate a shell profile, then click **Common Tasks**.
 - **Edit** to edit a shell profile, then click **Common Tasks**.
- Step 2** Complete the Shell Profile: Common Tasks page as described in [Table 9-9](#):

Table 9-9 *Shell Profile: Common Tasks*

Option	Description
Privilege Level	
Default Privilege	<p>(Optional) Enables the initial privilege level assignment that you allow for a client, through shell authorization. If disabled, the setting is not interpreted in authorization and permissions.</p> <p>The Default Privilege Level specifies the default (initial) privilege level for the shell profile. If you select Static as the Enable Default Privilege option, you can select the default privilege level; the valid options are 0 to 15.</p> <p>If you select Dynamic as the Enable Default Privilege option, you can select attribute from dynamic ACS dictionary, for a substitute attribute.</p>

Table 9-9 Shell Profile: Common Tasks

Option	Description
Maximum Privilege	<p>(Optional) Enables the maximum privilege level assignment for which you allow a client after the initial shell authorization.</p> <p>The Maximum Privilege Level specifies the maximum privilege level for the shell profile. If you select the Enable Change of Privilege Level option, you can select the maximum privilege level; the valid options are 0 to 15.</p> <p>If you choose both default and privilege level assignments, the default privilege level assignment must be equal to or lower than the maximum privilege level assignment.</p>
Shell Attributes	
Select Not in Use for the options provided below if you do not want to enable them.	
If you select Dynamic , you can substitute the static value of a TACACS+ attribute with a value of another attribute from one of the listed dynamic dictionaries	
Access Control List	<p>(Optional) Choose Static to specify the name of the access control list to enable it. The name of the access control list can be up to 27 characters, and cannot contain the following:</p> <p>A hyphen (-), left bracket ([), right bracket (]), forward slash (/), back slash (\), apostrophe ('), left angle bracket (<), or right angle bracket (>).</p> <p>Choose Dynamic to select attribute from dynamic ACS dictionary, for a substitute attribute.</p>
Auto Command	<p>(Optional) Choose Static and specify the command to enable it.</p> <p>Choose Dynamic to select attribute from dynamic ACS dictionary, for a substitute attribute.</p>
No Callback Verify	<p>(Optional) Choose Static to specify whether or not you want callback verification. Valid options are:</p> <ul style="list-style-type: none"> • True—Specifies that callback verification is not needed. • False—Specifies that callback verification is needed. <p>Choose Dynamic to select attribute from dynamic ACS dictionary, for a substitute attribute.</p>
No Escape	<p>(Optional) Choose Static to specify whether or not you want escape prevention. Valid options are:</p> <ul style="list-style-type: none"> • True—Specifies that escape prevention is enabled. • False—Specifies that escape prevention is not enabled. <p>Choose Dynamic to select attribute from dynamic ACS dictionary, for a substitute attribute.</p>
No Hang Up	<p>(Optional) Choose Static to specify whether or not you want any hangups. Valid options are:</p> <ul style="list-style-type: none"> • True—Specifies no hangups are allowed. • False—Specifies that hangups are allowed. <p>Choose Dynamic to select attribute from dynamic ACS dictionary, for a substitute attribute.</p>
Timeout	<p>(Optional) Choose Static to enable and specify, in minutes, the duration of the allowed timeout in the value field. The valid range is from 0 to 999.</p> <p>Choose Dynamic to select attribute from dynamic ACS dictionary, for a substitute attribute.</p>
Idle Time	<p>(Optional) Choose Static to enable and specify, in minutes, the duration of the allowed idle time in the value field. The valid range is from 0 to 999.</p> <p>Choose Dynamic to select attribute from dynamic ACS dictionary, for a substitute attribute.</p>

Table 9-9 Shell Profile: Common Tasks

Option	Description
Callback Line	(Optional) Choose Static to enable and specify the callback phone line in the value field. Choose Dynamic to select attribute from dynamic ACS dictionary, for a substitute attribute.
Callback Rotary	(Optional) Choose Static to enable and specify the callback rotary phone line in the value field. Choose Dynamic to select attribute from dynamic ACS dictionary, for a substitute attribute.

Step 3 Click:

- **Submit** to save your changes and return to the Shell Profiles page.
- The **General** tab to configure the name and description for the authorization profile; see [Defining General Shell Profile Properties, page 9-24](#).
- The **Custom Attributes** tab to configure Custom Attributes for the authorization profile; see [Defining Custom Attributes, page 9-27](#).

To substitute the static value of a TACACS+ attribute with a value of another attribute from one of the listed dynamic dictionaries, complete the following steps.

- Step 1** Choose **System Administration > Configuration > Dictionaries > Identity > Internal Users** to add attributes to the Internal Users Dictionary.
- Step 2** Choose **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles** to create a Shell Profile.
- Step 3** Choose **Custom Attributes** tab to create a new attribute and choose **Dynamic** as Attribute Value and correlate it to created attribute in Internal Users Dictionary.
- Step 4** Create a new rule in **Access Policies > Access Services > Default Device Admin > Authorization** and choose the Results created as Shell Profile instead.
- After authorization you will see the response as dynamic attribute value from Internal ID Store.

Related Topics

- [Defining Custom Attributes, page 9-27](#)
- [Configuring Shell/Command Authorization Policies for Device Administration, page 10-36](#)

Defining Custom Attributes

Use this tab to define custom attributes for the shell profile. This tab also displays the Common Tasks Attributes that you have chosen in the Common Tasks tab.

- Step 1** Edit the fields in the Custom Attributes tab as described in [Table 9-10](#):

Table 9-10 Shell Profile: Custom Attributes Page

Option	Description
Common Tasks Attributes	Displays the names, requirements, and values for the Common Tasks Attributes that you have defined in the Common Tasks tab.
Manually Entered	Use this section to define custom attributes to include in the authorization profile. As you define each attribute, its name, requirement, and value appear in the table. To: <ul style="list-style-type: none"> Add a custom attribute, fill in the fields below the table and click Add. Edit a custom attribute, select the appropriate row in the table and click Edit. <p>The custom attribute parameters appear in the fields below the table. Edit as required, then click Replace.</p>
Attribute	Name of the custom attribute.
Requirement	Choose whether this custom attribute is Mandatory or Optional.
Attribute Value	Choose whether the custom attribute is Static or Dynamic.

Step 2 Click:

- **Submit** to save your changes and return to the Shell Profiles page.
- The **General** tab to configure the name and description for the authorization profile; see [Defining General Shell Profile Properties, page 9-24](#).
- The **Common Tasks** tab to configure the shell profile's privilege level and attributes for the authorization profile; see [Defining Common Tasks, page 9-25](#).

Related Topics

- [Defining General Shell Profile Properties, page 9-24](#)
- [Defining Common Tasks, page 9-25](#)

Creating, Duplicating, and Editing Command Sets for Device Administration

Command sets provide decisions for allowed commands and arguments for device administration. You can specify command sets as results in a device configuration authorization policy. Shell profiles and command sets are combined for authorization purposes, and are enforced for the duration of a user's session.

You can duplicate a command set if you want to create a new command set that is the same, or similar to, an existing command set. After duplication is complete, you access each command set (original and duplicated) separately to edit or delete them.

After you create command sets, you can use them in authorizations and permissions within rule tables. A rule can contain multiple command sets. See [Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-23](#).

**Note**

Command sets support TACACS+ protocol attributes only.

To create, duplicate, or edit a new command set:

- Step 1** Choose **Policy Elements > Authorization and Permissions > Device Administration > Command Sets**.
- The Command Sets page appears.
- Step 2** Do one of the following:
- Click **Create**.
The Command Set Properties page appears.
 - Check the check box the command set that you want to duplicate and click **Duplicate**.
The Command Set Properties page appears.
 - Click the name that you want to modify; or, check the check box the name that you want to modify and click **Edit**.
The Command Set Properties page appears.
 - Click **File Operations** to perform any of the following functions:
 - Add—Choose this option to add command sets from the import file to ACS.
 - Update—Choose this option to replace the list of command sets in ACS with the list of command sets in the import file.
 - Delete—Choose this option to delete the command sets listed in the import file from ACS.
- See [Performing Bulk Operations for Network Resources and Users, page 7-8](#) for a detailed description of the bulk operations.
- Click **Export** to export the command sets from ACS to your local hard disk.
A dialog box appears, prompting you to enter an encryption password to securely export the command sets:
 - Check the **Password** check box and enter the password to encrypt the file during the export process, then click **Start Export**.
 - Click **Start Export** to export the command sets without any encryption.
- Step 3** Enter valid configuration data in the required fields.
- As a minimum configuration, you must enter a unique name for the command set; all other fields are optional. You can define commands and arguments; you can also add commands and arguments from other command sets.
- See [Table 9-11](#) for a description of the fields in the Command Set Properties page.

Table 9-11 *Command Set Properties Page*

Field	Description
Name	Name of the command set.
Description	(Optional) The description of the command set.
Permit any command that is not in the table below	Check to allow all commands that are requested, unless they are explicitly denied in the Grant table. Uncheck to allow only commands that are explicitly allowed in the Grant table.

Table 9-11 Command Set Properties Page (continued)

Field	Description
Command Set table	<p>Use this section to define commands to include in the authorization profile. As you define each command, its details appear in the table. To:</p> <ul style="list-style-type: none"> • Add a command, fill in the fields below the table and click Add. • Edit a command, select the appropriate row in the table, and click Edit. The command parameters appear in the fields below the table. Edit as required, then click Replace. <p>The order of commands in the Command Set table is important; policy rule table processing depends on which command and argument are matched first to make a decision on policy result choice. Use the control buttons at the right of the Command Set table to order your commands.</p>
Grant	<p>Choose the permission level of the associated command. Options are:</p> <ul style="list-style-type: none"> • Permit—The associated command and arguments are automatically granted. • Deny—The associated command and arguments are automatically denied. • Deny Always—The associated command and arguments are always denied.
Command	<p>Enter the command name. This field is not case sensitive. You can use the asterisk (*) to represent zero (0) or more characters in the command name, and you can use the question mark (?) to represent a single character in a command name.</p> <p>Examples of valid command name entries:</p> <ul style="list-style-type: none"> • SHOW • sH* • sho? • Sh*?
Arguments (field)	<p>Enter the argument associated with the command name. This field is not case sensitive. ACS 5.8.1 uses standard UNIX-type regular expressions.</p>
Select Command/Arguments from Command Set	<p>To add a command from another command set:</p> <ol style="list-style-type: none"> 1. Choose the command set. 2. Click Select to open a page that lists the available commands and arguments. 3. Choose a command and click OK.

Step 4 Click **Submit**.

The command set is saved. The Command Sets page appears with the command set that you created or duplicated.

Related Topics

- [Creating, Duplicating, and Editing Authorization Profiles for Network Access, page 9-18](#)
- [Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-23](#)
- [Deleting an Authorizations and Permissions Policy Element, page 9-32](#)
- [Creating, Duplicating, and Editing a Shell Profile for Device Administration, page 9-23](#)

Creating, Duplicating, and Editing Downloadable ACLs

You can define downloadable ACLs 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 downloadable ACLs 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 downloadable ACL if you want to create a new downloadable ACL that is the same, or similar to, an existing downloadable ACL.

After duplication is complete, you access each downloadable ACL (original and duplicated) separately to edit or delete them.

To create, duplicate or edit a downloadable ACL:

-
- Step 1** Choose **Policy Elements > Authorization and Permissions > Named Permission Objects > Downloadable ACLs**.
- The Downloadable ACLs page appears.
- Step 2** Do one of the following:
- Click **Create**.
The Downloadable ACL Properties page appears.
 - Check the check box the downloadable ACL that you want to duplicate and click **Duplicate**.
The Downloadable ACL Properties page appears.
 - Click the name that you want to modify; or, check the check box the name that you want to modify and click **Edit**.
The Downloadable ACL Properties page appears.
 - Click **File Operations** to perform any of the following functions:
 - Add—Choose this option to add ACLs from the import file to ACS.
 - Update—Choose this option to replace the list of ACLs in ACS with the list of ACLs in the import file.
 - Delete—Choose this option to delete the ACLs listed in the import file from ACS.
- See [Performing Bulk Operations for Network Resources and Users, page 7-8](#) for a detailed description of the bulk operations.
- Click **Export** to export the DACLS from ACS to your local hard disk.
A dialog box appears, prompting you to enter an encryption password to securely export the DACLS:
 - Check the **Password** check box and enter the password to encrypt the file during the export process, then click **Start Export**.
 - Click **Start Export** to export the DACLS without any encryption.
- Step 3** Enter valid configuration data in the required fields as shown in [Table 9-12](#), and define one or more ACLs by using standard ACL syntax.

Table 9-12 Downloadable ACL Properties Page

Option	Description
Name	Name of the DACL.
Description	Description of the DACL.
Downloadable ACL Content	<p>Define the ACL content.</p> <p>Use standard ACL command syntax and semantics. The ACL definitions comprise one or more ACL commands; each ACL command must occupy a separate line.</p> <p>For detailed ACL definition information, see the command reference section of your device configuration guide.</p>

Step 4 Click **Submit**.

The downloadable ACL is saved. The Downloadable ACLs page appears with the downloadable ACL that you created or duplicated.

Related Topics

- [Creating, Duplicating, and Editing Authorization Profiles for Network Access, page 9-18](#)
- [Configuring a Session Authorization Policy for Network Access, page 10-31](#)
- [Deleting an Authorizations and Permissions Policy Element, page 9-32](#)

Deleting an Authorizations and Permissions Policy Element

To delete an authorizations and permissions policy element:

Step 1 Choose **Policy Elements > Authorization and Permissions**; then, navigate to the required option.

The corresponding page appears.

Step 2 Check one or more check boxes the items that you want to delete and click **Delete**.

The following message appears:

Are you sure you want to delete the selected item/items?

Step 3 Click **OK**.

The page appears without the deleted object.

Configuring Security Group Access Control Lists

Security group access control lists (SGACLs) are applied at Egress, based on the source and destination SGTs. Use this page to view, create, duplicate and edit SGACLs. When you modify the name or content of an SGACL, ACS updates its generation ID. When the generation ID of an SGACL changes, the relevant Security Group Access network devices reload the content of the SGACL.

SGACLs are also called role-based ACLs (RBACLs).

- Step 1** Choose **Policy Elements > Authorizations and Permissions > Named Permissions Objects > Security Group ACLs**.

The Security Group Access Control Lists page appears with the fields described in [Table 9-13](#):

Table 9-13 Security Group Access Control Lists Page

Option	Description
Name	The name of the SGACL.
Description	The description of the SGACL.

- Step 2** Click one of the following options:
- **Create** to create a new SGACL.
 - **Duplicate** to duplicate an SGACL.
 - **Edit** to edit an SGACL.

- Step 3** Complete the fields in the Security Group Access Control Lists Properties page as described in [Table 9-14](#):

Table 9-14 Security Group Access Control List Properties Page

Option	Description
General	
Name	Name of the SGACL. You cannot use spaces, hyphens (-), question marks (?), or exclamation marks (!) in the name. After you create an SGACL, its generation ID appears.
Generation ID	<i>Display only.</i> ACS updates the generation ID of the SGACL if you change the: <ul style="list-style-type: none"> • Name of the SGACL. • Content of the SGACL (the ACEs). Changing the SGACL description does not affect the generation ID.
Description	Description of the SGACL.
Security Group ACL Content	Enter the ACL content. Ensure that the ACL definition is syntactically and semantically valid.

- Step 4** Click **Submit**.



Managing Access Policies

In ACS 5.8.1, policy drives all activities. Policies consist mainly of rules that determine the action of the policy. You create access services to define authentication and authorization policies for requests. A global service selection policy contains rules that determine which access service processes an incoming request.

For a basic work flow for configuring policies and all their elements, see [Flows for Configuring Services and Policies, page 3-19](#). In general, before you can configure policy rules, you must configure all the elements that you will need, such as identities, conditions, and authorizations and permissions.

For information about:

- Managing identities, see [Managing Users and Identity Stores, page 8-1](#)
- Configuring conditions, see [Managing Policy Elements, page 9-1](#).
- Configuring authorizations and permissions, see [17, page 17-1](#).

This section contains the following topics:

- [Policy Creation Flow, page 10-1](#)
- [Customizing a Policy, page 10-4](#)
- [Configuring the Service Selection Policy, page 10-5](#)
- [Configuring Access Services, page 10-11](#)
- [Configuring Access Service Policies, page 10-23](#)
- [Configuring Compound Conditions, page 10-41](#)
- [Security Group Access Control Pages, page 10-47](#)
- [Maximum User Sessions, page 10-52](#)
- [Maximum Login Failed Attempts Policy, page 10-57](#)

For information about creating Egress and NDAC policies for Cisco Security Group Access, see [Configuring an NDAC Policy, page 4-24](#).

Policy Creation Flow

Policy creation depends on your network configuration and the degree of refinement that you want to bring to individual policies. The endpoint of policy creation is the access service that runs as the result of the service selection policy. Each policy is rule driven.

In short, you must determine the:

- Details of your network configuration.
- Access services that implement your policies.
- Rules that define the conditions under which an access service can run.

This section contains the following topics:

- [Network Definition and Policy Goals, page 10-2](#)
- [Policy Elements in the Policy Creation Flow, page 10-2](#)
- [Access Service Policy Creation, page 10-4](#)
- [Service Selection Policy Creation, page 10-4](#)

Network Definition and Policy Goals

The first step in creating a policy is to determine the devices and users for which the policy should apply. Then you can start to configure your policy elements.

For basic policy creation, you can rely on the order of the drawers in the left navigation pane of the web interface. The order of the drawers is helpful because some policy elements are dependent on other policy elements. If you use the policy drawers in order, you initially avoid having to go backward to define elements that your current drawer requires.

For example, you might want to create a simple device administration policy from these elements in your network configuration:

- Devices—Routers and switches.
- Users—Network engineers.
- Device Groups—Group devices by location and separately by device type.
- Identity groups—Group network engineers by location and separately by access level.

The results of the policy apply to the administrative staff at each site:

- Full access to devices at their site.
- Read-only access to all other devices.
- Full access to everything for a supervisor.

The policy itself applies to network operations and the administrators who will have privileges within the device administration policy. The users (network engineers) are stored in the internal identity store.

The policy results are the authorizations and permissions applied in response to the access request. These authorizations and permissions are also configured as policy elements.

Policy Creation Flow—Next Steps

- [Policy Elements in the Policy Creation Flow, page 10-2](#)
- [Access Service Policy Creation, page 10-4](#)
- [Service Selection Policy Creation, page 10-4](#)

Policy Elements in the Policy Creation Flow

The web interface provides these defaults for defining device groups and identity groups:

- All Locations

- All Device Types
- All Groups

The locations, device types, and identity groups that you create are children of these defaults.

To create the building blocks for a basic device administration policy:

-
- Step 1** Create network resources. In the Network Resources drawer, create:
- Device groups for Locations, such as All Locations > East, West, HQ.
 - Device groups for device types, such as All Device Types > Router, Switch.
 - AAA clients (clients for AAA switches and routers, address for each, and protocol for each), such as EAST-ACCESS-SWITCH, HQ-CORE-SWITCH, or WEST-WAN-ROUTER.
- Step 2** Create users and identity stores. In the Users and Identity Stores drawer, create:
- Identity groups (Network Operations and Supervisor).
 - Specific users and association to identity groups (Names, Identity Group, Password, and more).
- Step 3** Create authorizations and permissions for device administration. In the Policy Elements drawer, create:
- Specific privileges (in Shell Profiles), such as full access or read only.
 - Command Sets that allow or deny access (in Command Sets).
-

For this policy, you now have the following building blocks:

- Network Device Groups (NDGs), such as:
 - Locations—East, HQ, West.
 - Device Types—Router, Switch.
- Identity groups, such as:
 - Network Operations Sites—East, HQ, West.
 - Access levels—Full Access.
- Devices—Routers and switches that have been assigned to network device groups.
- Users—Network engineers in the internal identity store that have been assigned to identity groups.
- Shell Profiles—Privileges that can apply to each administrator, such as:
 - Full privileges.
 - Read only privileges.
- Command Sets—Allow or deny authorization to each administrator.

Policy Creation Flow—Previous Step

- [Network Definition and Policy Goals, page 10-2](#)

Policy Creation Flow—Next Steps

- [Access Service Policy Creation, page 10-4](#)
- [Service Selection Policy Creation, page 10-4](#)

Access Service Policy Creation

After you create the basic elements, you can create an access policy that includes identity groups and privileges. For example, you can create an access service for device administration, called NetOps, which contains authorization and authentication policies that use this data:

- Users in the Supervisor identity group—Full privileges to all devices at all locations.
- User in the East, HQ, West identity groups—Full privileges to devices in the corresponding East, HQ, West device groups.
- If no match—Deny access.

Policy Creation Flow—Previous Steps

- [Network Definition and Policy Goals, page 10-2](#)
- [Policy Elements in the Policy Creation Flow, page 10-2](#)

Policy Creation Flow—Next Step

- [Service Selection Policy Creation, page 10-4](#)

Service Selection Policy Creation

ACS provides support for various access use cases; for example, device administration, wireless access, network access control, and so on. You can create access policies for each of these use cases. Your service selection policy determines which access policy applies to an incoming request.

For example, you can create a service selection rule to apply the NetOps access service to any access request that uses the TACAC+ protocol.

Policy Creation Flow—Previous Steps

- [Network Definition and Policy Goals, page 10-2](#)
- [Policy Elements in the Policy Creation Flow, page 10-2](#)
- [Access Service Policy Creation, page 10-4](#)

Customizing a Policy

ACS policy rules contain conditions and results. Before you begin to define rules for a policy, you must configure which types of conditions that policy will contain. This step is called customizing your policy. The condition types that you choose appear on the Policy page. You can apply only those types of conditions that appear on the Policy page. For information about policy conditions, see [Managing Policy Conditions, page 9-1](#).

By default, a Policy page displays a single condition column for compound expressions. For information on compound conditions, see [Configuring Compound Conditions, page 10-41](#).

If you have implemented Security Group Access functionality, you can also customize results for authorization policies.

**Caution**

If you have already defined rules, be certain that a rule is not using any condition that you remove when customizing conditions. Removing a condition column removes all configured conditions that exist for that column.

To customize a policy:

Step 1

Open the Policy page that you want to customize. For:

- The service selection policy, choose **Access Policies > Service Selection Policy**.
- An access service policy, choose **Access Policies > Access Services > *service* > *policy***, where *service* is the name of the access service, and *policy* is the name of the policy that you want to customize.

Step 2

In the Policy page, click **Customize**.

A list of conditions appears. This list includes identity attributes, system conditions, and custom conditions.

**Note**

Identity-related attributes are not available as conditions in a service selection policy.

Step 3

Move conditions between the Available and Selected list boxes.

Step 4

Click **OK**

The selected conditions now appear under the Conditions column.

Step 5

Click **Save Changes**.

Configuring a Policy—Next Steps

- [Configuring the Service Selection Policy, page 10-5](#)
- [Configuring Access Service Policies, page 10-23](#)

Configuring the Service Selection Policy

The service selection policy determines which access service processes incoming requests. You can configure a simple policy, which applies the same access service to all requests; or, you can configure a rule-based service selection policy.

In the rule-based policy, each service selection rule contains one or more conditions and a result, which is the access service to apply to an incoming request. You can create, duplicate, edit, and delete rules within the service selection policy, and you can enable and disable them.

This section contains the following topics:

- [Configuring a Simple Service Selection Policy, page 10-6](#)
- [Creating, Duplicating, and Editing Service Selection Rules, page 10-8](#)

**Note**

If you create and save a simple policy, and then change to a rule-based policy, the simple policy becomes the default rule of the rule-based policy. If you have saved a rule-based policy and then change to a simple policy, you will lose all your rules except for the default rule. ACS automatically uses the default rule as the simple policy.

Configuring a Simple Service Selection Policy

A simple service selection policy applies the same access service to all requests.

To configure a simple service selection policy:

-
- Step 1** Select **Access Policies > Service Selection Policy**.
By default, the Simple Service Selection Policy page appears.
- Step 2** Select an access service to apply; or, choose **Deny Access**.
- Step 3** Click **Save Changes** to save the policy.
-

Service Selection Policy Page

Use this page to configure a simple or rule-based policy to determine which service to apply to incoming requests.


To display this page, choose **Access Policies > Service Selection**.

If you have already configured the service selection policy, the corresponding Simple Policy page (see [Table 10-1](#)) or Rule-based Policy page (see [Table 10-2](#)) opens; otherwise, the Simple Policy page opens by default.

Table 10-1 *Simple Service Selection Policy Page*

Option	Description
Policy type	<p>Defines the type of policy:</p> <ul style="list-style-type: none"> Select one result—The results apply to all requests. <p>Rule-based result selection—Configuration rules apply different results depending on the request.</p>
Service Selection Policy	Access service to apply to all requests. The default is Deny Access.

Table 10-2 Rule-based Service Selection Policy Page

Option	Description
Policy type	<p>Defines the type of policy to configure:</p> <ul style="list-style-type: none"> Select one result—Results apply to all requests. Rule-based result selection—Configuration rules apply different results depending on the request.
Status	<p>Current status of the rule that drives service selection. The rule statuses are:</p> <ul style="list-style-type: none"> Enabled—The rule is active. Disabled—ACS does not apply the results of the rule. Monitor Only—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	Rule name.
Conditions	<p>Conditions that determine the scope of the service. This column displays all current conditions in subcolumns.</p> <p>You cannot use identity-based conditions in a service selection rule.</p>
Results	Service that runs as a result of the evaluation of the rule.
Hit Count	Number of times that the rule is matched. Click Hit Count to refresh and reset this column.
Default Rule	<p>ACS applies the Default rule when:</p> <ul style="list-style-type: none"> Enabled rules are not matched. No other rules are defined. <p>Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.</p>
Customize button	<p>Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add.</p> <div>  <p>Caution If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.</p> </div>
Hit Count button	<p>Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.</p>

To configure a rule-based service selection policy, see these topics:

- [Creating, Duplicating, and Editing Service Selection Rules, page 10-8](#)
- [Deleting Service Selection Rules, page 10-10](#)

After you configure your service selection policy, you can continue to configure your access service policies. See [Configuring Access Service Policies, page 10-23](#).

Creating, Duplicating, and Editing Service Selection Rules

Create service selection rules to determine which access service processes incoming requests. The Default Rule provides a default access service in cases where no rules are matched or defined.

When you create rules, remember that the order of the rules is important. When ACS encounters a match as it processes the request of a client that tries to access the ACS network, all further processing stops and the associated result of that match is found. No further rules are considered after a match is found.

You can duplicate a service selection rule to create a new rule that is the same, or very similar to, an existing rule. The duplicate rule name is based on the original rule with parentheses to indicate duplication; for example, Rule-1(1). After duplication is complete, you access each rule (original and duplicated) separately. You cannot duplicate the Default rule.

You can edit all values of service selection rules; you can edit the specified access service in the Default rule.



Note

To configure a simple policy to apply the same access service to all requests, see [Configuring a Simple Service Selection Policy, page 10-6](#).

Before You Begin

- Configure the conditions that you want to use in the service selection policy. See [Managing Policy Conditions, page 9-1](#).



Note

Identity-related attributes are not available as conditions in a service selection policy.

- Create the access services that you want to use in the service selection policy. See [Creating, Duplicating, and Editing Access Services, page 10-12](#). You do not need to configure policies in the access service before configuring the service selection policy.
- Configure the types of conditions to use in the policy rules. See [Customizing a Policy, page 10-4](#), for more information.

To create, duplicate, or edit a service selection policy rule:

-
- Step 1** Select **Access Policies > Service Selection Policy**. If you:
- Previously created a rule-based policy, the Rule-Based Service Selection Policy page appears with a list of configured rules.
 - Have not created a rule-based policy, the Simple Service Selection Policy page appears. Click **Rule-Based**.
- Step 2** Do one of the following:
- Click **Create**.
 - Check the check box the rule that you want to duplicate; then click **Duplicate**.
 - Click the rule name that you want to modify; or, check the check box the name and click **Edit**.
- The Rule page appears.
- Step 3** Enter or modify values:
- User-defined rules—You can edit any value. Ensure that you include at least one condition. If you are duplicating a rule, you must change the rule name.

- The Default Rule—You can change only the access service.

See [Table 10-3](#) for field descriptions:

Table 10-3 *Service Selection Rule Properties Page*

Option	Description
General	
Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Status	Rule statuses are: <ul style="list-style-type: none"> • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor Only—The rule is active but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The Monitor option is especially useful for watching the results of a new rule.
Conditions	
conditions	Conditions that you can configure for the rule. By default, the compound condition appears. Click Customize in the Policy page to change the conditions that appear. The default value for each condition is <i>ANY</i> . To change the value for a condition, check the condition check box, then specify the value. If you check Compound Condition , an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-41 . Note The Service selection policy, which contains a compound condition with TACACS+ username, does not work consistently. The policy works only when the first TACACS+ authentication request contains a username. If the first packet does not have the username and when ACS requests NAS for the username, the TACACS+ username condition is not matched. Therefore, the request meets the default deny access condition and fails to meet the proper access service. It is recommended to use the other TACACS+ attributes such as remote address, existing in the first request, to the rule condition.
Results	
Service	Name of the access service that runs as a result of the evaluation of the rule.

Step 4 Click **OK**.

The Service Selection Policy page appears with the rule that you configured.

Step 5 Click **Save Changes**.

Related Topics

- [Configuring Access Services, page 10-11](#)
- [Deleting Service Selection Rules, page 10-10](#)

Displaying Hit Counts

Use this page to reset and refresh the Hit Count display on the Rule-based Policy page.

To display this page, click **Hit Count** on the Rule-based Policy page.

Table 10-4 Hit Count Page

Option	Description
Hit Counts Reset	
Last time hit counts were reset for this policy	Displays the date and time of the last hit count reset for this policy.
Reset hit counts display for this policy	Click Reset to reset the hit counts display to zero (0) for all rules on the Policy page.
Hit Counts Collection	
Hit counts are collected every:	Displays the interval between hit count collections.
Last time hit counts were collected for this policy:	Displays the date and time of the last hit count update for this policy.
Refresh hit counts display for this policy	Click Refresh to refresh the hit count display in the Policy page with updated hit counts for all rules. The previous hit counts are deleted. When a TACACS+ authentication request succeeds, the hit counts of the corresponding identity policy rule and authorization policy rule both increase by 1.

Deleting Service Selection Rules



Note You cannot delete the Default service selection rule.

To delete a service selection rule:

- Step 1** Select **Access Policies > Service Selection Policy**.
The Service Selection Policy page appears, with a list of configured rules.
- Step 2** Check one or more check boxes the rules that you want to delete.
- Step 3** Click **Delete**.
The Service Selection Rules page appears without the deleted rule(s).
- Step 4** Click **Save Changes** to save the new configuration.

Configuring Access Services

Access services contain the authentication and authorization policies for requests. You can create separate access services for different use cases; for example, device administration, wireless network access, and so on.

When you create an access service, you define the type of policies and policy structures that it contains; for example, policies for device administration or network access.

**Note**

You must create access services before you define service selection rules, although you do not need to define the policies in the services.

This section contains the following topics:

- [Creating, Duplicating, and Editing Access Services, page 10-12](#)
- [Deleting an Access Service, page 10-22](#)

After you create an access service, you can use it in the service selection policy. See [Configuring the Service Selection Policy, page 10-5](#).

You can customize and modify the policies in the access service. See [Configuring Access Service Policies, page 10-23](#).

Related Topic

- [Creating, Duplicating, and Editing Access Services, page 10-12](#)

Editing Default Access Services

ACS 5.8.1 is preconfigured with two default access services, one for device administration and another for network access. You can edit these access services.

To edit the default access service:

Step 1 Choose one of the following:

- **Access Policies > Access Services > Default Device Admin**
- **Access Policies > Access Services > Default Network Access**

The Default *Service* Access Service Edit page appears.

Step 2 Edit the fields in the Default *Service* Access Service page.

[Table 10-5](#) describes the fields in the General tab.

Table 10-5 *Default Access Service - General Page*

Option	Description
General	
Name	Name of the access service.
Description	Description of the access service.
Service Type	(Display only) Type of service, device administration, or network access.
Policy Structure	

Table 10-5 *Default Access Service - General Page*

Option	Description
Identity	Check to include an identity policy in the access service, to define the identity store or stores that ACS uses for authentication and attribute retrieval.
Group Mapping	Check to include a group mapping policy in the access service, to map groups and attributes that are retrieved from external identity stores to the identity groups in ACS.
Authorization	Check to include an authorization policy in the access service, to apply: <ul style="list-style-type: none">• Authorization profiles for network access services.• Shell profiles and command sets for device administration services.

Step 3 Edit the fields in the Allowed Protocols tab as described in [Table 10-7](#).

Step 4 Click **Submit** to save the changes you have made to the default access service.

Creating, Duplicating, and Editing Access Services

Access services contain the authentication and authorization policies for requests.

When you create an access service, you define:

- Policy structure—The types of policies the service will contain. You can define these according to a service template, an existing service, or a use case.

A service can contain:

- An Identity policy—Defines which identity store to use for authentication.
- A group mapping policy—Defines the identity group to which to map.
- An Authorization policy—For network access, this policy defines which session authorization profile to apply; for device administration, it defines which shell profile or command set to apply.
- Allowed protocols—Specifies which authentication protocols are allowed for this access service, and provides additional information about how ACS uses them for authentication.

Use a service template to define an access service with policies that are customized to use specific condition types. See [Configuring Access Services Templates, page 10-21](#) for information about the service templates.

Duplicate an access service to create a new access service with rules that are the same, or very similar to, an existing access service. After duplication is complete, you access each service (original and duplicated) separately.

To replicate a service policy structure without duplicating the source service's rules, create a new access service based on an existing service.

To create, duplicate, or edit an access service:

Step 1 Select **Access Policies > Access Services**.

The Access Services page appears with a list of configured services.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box the access service that you want to duplicate; then click **Duplicate**.
- Click the access service name that you want to modify; or, check the check box the name and click **Edit**.
- Click the access service name in the left navigation tab.

The Access Service Properties General page appears.

- If you are creating a new access service:
 - Define the name and policy structure of the access service.
 - Click **Next** to proceed to the Allowed Protocols page.
 - Click **Finish** to save the new access service.
- If you are duplicating or editing an access service:
 - Modify fields in the Properties page tabs as required. You can add policies, but you cannot remove existing policies.
 - Click **Submit** to save changes.

For information about valid field options, see:

- [Configuring General Access Service Properties, page 10-13](#)
- [Configuring Access Service Allowed Protocols, page 10-16](#)
- [Configuring Access Services Templates, page 10-21](#)

The access service configuration is saved. The Access Services page appears with the new configuration.

Related Topics

- [Deleting an Access Service, page 10-22](#)
- [Configuring Access Service Policies, page 10-23](#)
- [Configuring the Service Selection Policy, page 10-5](#)

Configuring General Access Service Properties

Access service definitions contain general and allowed protocol information. When you duplicate and edit services, the Access Service properties page contains tabs.

Step 1 Select **Access Policies > Access Services**, then click **Create**, **Duplicate**, or **Edit**.

Step 2 Complete the fields as described in [Table 10-6](#):

Table 10-6 Access Service Properties—General Page

Option	Description
General	
Name	Name of the access service. If you are duplicating a service, you must enter a unique name as a minimum configuration; all other fields are optional.

Table 10-6 Access Service Properties—General Page (continued)

Option	Description
Description	Description of the access service.
Access Service Policy Structure	
Based on service template	Creates an access service containing policies based on a predefined template. This option is available only for service creation.
Based on existing service	Creates an access service containing policies based on an existing access service. The new access service does not include the existing service's policy rules. This option is available only for service creation. To replicate a service, including its policy rules, duplicate an existing access service.
User selected service type	Provides you the option to select the access service type. The available options are Network Access, Device Administration, and External Proxy. The list of policies you can configure depends on your choice of access service type.
User Selected Service Type—Network Access and Device Administration	
Policy Structure	
Identity	Check to include an identity policy in the access service to define the identity store or stores that ACS uses for authentication and attribute retrieval.
Group Mapping	Check to include a group mapping policy in the access service to map groups and attributes that are retrieved from external identity stores to ACS identity groups.
Authorization	Check to include an authorization policy in the access service to apply: <ul style="list-style-type: none"> Authorization profiles for network access services. Shell profiles and command sets for device administration services.
User Selected Service Type—External Proxy	
External Proxy Servers—Select the set of external servers to be used for proxies. You can also determine the order in which these servers are used.	
Available External Proxy Servers	List of available external RADIUS and TACACS+ servers. Select the external servers to be used for proxy and move them to the Selected External Proxy Servers list.
Selected External Proxy Servers	List of selected external proxy servers.
Advanced Options	
Accounting	
Remote Accounting	Check to enable remote accounting.
Local Accounting	Check to enable local accounting.
Username Prefix\Suffix Stripping	
Strip start of subject name up to the first occurrence of the separator	Check to strip the username from the prefix. For example, if the subject name is acme\smith and the separator is \, the username becomes smith. The default separator is \.
Strip end of subject name from the last occurrence of the separator	Check to strip the username from the suffix. For example, if the subject name is smith@acme.com and the separator is @, the username becomes smith. The default separator is @.
RADIUS INBOUND Attributes Injection—The RADIUS INBOUND attributes section is used for manipulating the incoming attributes before sending them to the proxy server.	

Table 10-6 Access Service Properties—General Page (continued)

Option	Description
Add	After you define a RADIUS incoming attribute, click ADD to add it to the RADIUS attributes list.
Edit	To edit the listed RADIUS incoming attribute, select the attribute in the list and click Edit . The attribute properties appear in the fields. Modify the properties as required, then click Replace .
Replace	Click Replace to replace the selected RADIUS incoming attribute with the value that is currently defined in this field.
Delete	Click Delete to delete the selected RADIUS incoming attribute from the list.
Dictionary Type	Choose the dictionary that contains the RADIUS incoming attribute you want to use.
RADIUS Attribute	Name of the RADIUS attribute. Click Select to choose a RADIUS attribute from the specified dictionary.
Attribute Type	Type of the selected RADIUS attribute. Client vendor type of the attribute, from which ACS allows access requests. For a description of the attribute types, refer to Cisco IOS documentation for the Cisco IOS Software release that is running on your AAA clients.
Operation	<p>You can perform the following three operations:</p> <ul style="list-style-type: none"> Choose ADD to add a new attribute value for the selected RADIUS attribute: <ul style="list-style-type: none"> If Multiple not allowed—adds the new value for the selected attribute only if this attribute does not exist on the request. If Multiple allowed—always adds the attribute with a new value. Choose UPDATE to update the existing value of a selected RADIUS attribute: <ul style="list-style-type: none"> If Multiple not allowed—updates the attribute value with the new value if the attribute exists on the request. If Multiple allowed—removes all occurrences of this attribute and adds one attribute with the new value. If the attribute is a cisco-avpair (pair of key=value), the update is done according to the key. Choose DELETE to delete the value of the selected RADIUS attribute. <p>The attribute operations statements are ordered. The administrator can change the statement's order at the time of configuration. ACS performs the operation on the attributes according to the configured order. For more information on this, see RADIUS Attribute Rewrite Operation, page 4-29.</p>
Attribute New Value	Enter a new value for the selected RADIUS incoming attribute. This option is not available if you choose the delete operation.
RADIUS OUTBOUND Attributes Injection—The RADIUS OUTBOUND attributes section is used for manipulating the outgoing attributes before sending them from the proxy server.	
Add	After you define a RADIUS outgoing attribute, click ADD to add it to the RADIUS attributes list.
Edit	To edit the listed RADIUS outgoing attribute, select the attribute in the list and click Edit . The attribute properties appear in the fields. Modify the properties as required, then click Replace .
Replace	Click Replace to replace the selected RADIUS attribute with the value that is currently defined in this field.
Delete	Click Delete to delete the selected RADIUS outgoing attribute from the list.
Dictionary Type	Choose the dictionary that contains the RADIUS outgoing attribute you want to use.

Table 10-6 Access Service Properties—General Page (continued)

Option	Description
RADIUS Attribute	Name of the RADIUS attribute. Click Select to choose a RADIUS attribute from the specified dictionary.
Attribute Type	Type of the selected RADIUS attribute. Client vendor type of the attribute, from which ACS allows access requests. For a description of the attribute types, refer to Cisco IOS documentation for the Cisco IOS Software release that is running on your AAA clients.
Operation	<p>You can perform the following three operations:</p> <ul style="list-style-type: none"> Choose ADD to add a new attribute value for the selected RADIUS attribute: <ul style="list-style-type: none"> If Multiple not allowed—adds the new value for the selected attribute only if this attribute does not exist on the request. If Multiple allowed—always adds the attribute with a new value. Choose UPDATE to update the existing value of a selected RADIUS attribute: <ul style="list-style-type: none"> If Multiple not allowed—updates the attribute value with the new value if the attribute exists on the request. If Multiple allowed—removes all occurrences of this attribute and adds one attribute with the new value. If the attribute is a cisco-avpair (pair of key=value), the update is done according to the key. Choose DELETE to delete the value of the selected RADIUS attribute. <p>The attribute operations statements are ordered. The administrator can change the statement's order at the time of configuration. ACS performs the operation on the attributes according to the configured order. For more information on this, see RADIUS Attribute Rewrite Operation, page 4-29.</p>
Attribute New Value	Enter a new value for the selected RADIUS outgoing attribute. This option is not available if you choose the delete operation.

- Step 3** Click **Next** to configure the allowed protocols. See [Configuring Access Service Allowed Protocols, page 10-16](#).

Related Topic

- [Configuring Access Service Allowed Protocols, page 10-16](#)
- [Configuring Access Services Templates, page 10-21](#)

Configuring Access Service Allowed Protocols

The allowed protocols are the second part of access service creation. Access service definitions contain general and allowed protocol information. When you duplicate and edit services, the Access Service properties page contains tabs.

- Step 1** Select **Access Policies > Access Services**, and then click:
- **Create** to create a new access service, and then click **Next** to go to the Allowed Protocols screen.

- **Duplicate** to duplicate an access service, then click **Next** to go to the Allowed Protocols screen.
- **Edit** to edit an access service, then click **Next** to go to the Allowed Protocols screen.

Step 2 Complete the fields as shown in [Table 10-7](#):

Table 10-7 Access Service Properties—Allowed Protocols Page

Option	Description
Process Host Lookup	<p>Check to configure ACS to process the Host Lookup field (for example, when the RADIUS Service-Type equals 10) and use the System UserName attribute from the RADIUS Calling-Station-ID attribute.</p> <p>Uncheck for ACS to ignore the Host Lookup request and use the original value of the system UserName attribute for authentication and authorization. When unchecked, message processing is according to the protocol (for example, PAP).</p>
Authentication Protocols	
Allow PAP/ASCII	<p>Enables PAP/ASCII. PAP uses clear-text passwords (that is, unencrypted passwords) and is the least secure authentication protocol.</p> <p>When you check Allow PAP/ASCII, you can check Detect PAP as Host Lookup to configure ACS to detect this type of request as a Host Lookup (instead of PAP) request in the network access service.</p>
Allow CHAP	Enables CHAP authentication. CHAP uses a challenge-response mechanism with password encryption. CHAP does not work with the Windows Active Directory.
Allow MS-CHAPv1	Enables MS-CHAPv1.
Allow MSCHAPv2	Enables MSCHAPv2.
Allow EAP-MD5	<p>Enables EAP-based Message Digest 5 hashed authentication.</p> <p>When you check Allow EAP-MD5, you can check Detect EAP-MD5 as Host Lookup to configure ACS to detect this type of request as a Host Lookup (instead of EAP-MD5) request in the network access service.</p>
Allow EAP-TLS	<p>Enables the EAP-TLS Authentication protocol and configures EAP-TLS settings. You can specify how ACS verifies 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 ACS and the end-user client. If you choose Allow EAP-TLS, you can configure the following:</p> <ul style="list-style-type: none"> • Enable Stateless Session resume—Check this check box to enable the Stateless Session Resume feature per Access service. This feature enables you to configure the following options: <ul style="list-style-type: none"> – Proactive Session Ticket update—Enter the value as a percentage to indicate how much of the Time to Live must elapse before the session ticket is updated. For example, the session ticket update occurs after 10 percent of the Time to Live has expired, if you enter the value 10. – Session ticket Time to Live—Enter the equivalent maximum value in days, weeks, months, and years, using a positive integer. <p>EAP-TLS is a certificate-based authentication protocol. EAP-TLS authentication can occur only after you have completed the required steps to configure certificates. See Configuring Local Server Certificates, page 18-16 for more information.</p>
Allow LEAP	Enables LEAP authentication.

Table 10-7 Access Service Properties—Allowed Protocols Page (continued)

Option	Description
Allow PEAP	<p>Enables the PEAP authentication protocol and PEAP settings. The default inner method is MSCHAPv2.</p> <p>When you check Allow PEAP, you can configure the following PEAP inner methods:</p> <ul style="list-style-type: none"> • Allow EAP-TLS—Check to use EAP-TLS as the inner method. • Allow EAP-MSCHAPv2—Check to use EAP-MSCHAPv2 as the inner method. <ul style="list-style-type: none"> – Allow Password Change—Check for ACS to support password changes. – Retry Attempts—Specifies how many times ACS requests user credentials before returning login failure. Valid values are 1 to 3. • Allow EAP-GTC—Check to use EAP-GTC as the inner method. <ul style="list-style-type: none"> – Allow Password Change—Check for ACS to support password changes. – Retry Attempts—Specifies how many times ACS requests user credentials before returning login failure. Valid values are 1 to 3. • Allow PEAP Cryptobinding TLV—Check to use the PEAP cryptobinding TLV support. • Allow PEAPv0 only for legacy clients—Check this option to allow PEAP supplicants to negotiate PEAPv0 only. <p>Note A few legacy clients do not confirm the PEAPv1 protocol standard. As a result, the EAP conversations are dropped with an <code>Invalid EAP payload</code> error message.</p>

Table 10-7 Access Service Properties—Allowed Protocols Page (continued)

Option	Description
Allow EAP-FAST	<p>Enables the 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 MSCHAPv2.</p> <p>When you check Allow EAP-FAST, you can configure EAP-FAST inner methods:</p> <ul style="list-style-type: none"> • Allow EAP-MSCHAPv2 <ul style="list-style-type: none"> – Allow Password Change—Check for ACS to support password changes in phase zero and phase two of EAP-FAST. – Retry Attempts—Specifies how many times ACS requests user credentials before returning login failure. Valid values are 1-3. • Allow EAP-GTC <ul style="list-style-type: none"> – Allow Password Change—Check for ACS to support password changes in phase zero and phase two of EAP-FAST. – Retry Attempts—Specifies how many times ACS requests user credentials before returning login failure. Valid values are 1-3. • Allow TLS-Renegotiation—Check for ACS to support TLS-Renegotiation. This option allows an anonymous TLS handshake between the end-user client and ACS. EAP-MS-CHAP will be used as the only inner method in phase zero. • Use PACs—Choose to configure ACS to provision authorization PACs for EAP-FAST clients. Additional PAC Options, page 10-20 appear. • Don't use PACs—Choose to configure ACS to use EAP-FAST without issuing or accepting any tunnel or machine PACs. All requests for PACs are ignored and ACS responds with a Success-TLV without a PAC. <ul style="list-style-type: none"> – Allow Machine Authentication—Check this option to configure ACS to perform machine authentication. – Accept Client Certificate—Check this option to configure ACS to accept client certificates when you use Cisco IP phones.

Table 10-7 Access Service Properties—Allowed Protocols Page (continued)

Option	Description
Allow EAP-FAST (continued)	<p>PAC Options</p> <ul style="list-style-type: none"> 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 one (1) day. Proactive PAC Update When: <n%> of PAC TTL is Left—The Update value ensures that the client has a valid PAC. ACS initiates 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. (Default: 10%) Allow Anonymous In-band PAC Provisioning—Check for ACS to establish a secure anonymous TLS handshake with the client and provision it with a so-called PAC by using phase zero of EAP-FAST with EAP-MSCHAPv2. <p>Note To enable Anonymous PAC Provisioning, you must choose both the inner methods, EAP-MSCHAPv2 and EAP-GTC.</p> <ul style="list-style-type: none"> Allow Authenticated In-band PAC Provisioning—ACS uses Secure Socket Layer (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 ACS. <ul style="list-style-type: none"> Server Returns Access Accept After Authenticated Provisioning—Check this option to configure ACS to return an Access-Accept message to the client after successful authenticated PAC provisioning. Accept Client Certificate For Provisioning—Check this option to configure ACS to accept client certificates for PAC provisioning when you use Cisco IP phones. Allow Machine Authentication—Check for ACS 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). <p>The machine PAC can be provisioned to the client by request (in-band) or by administrator (out-of-band). When ACS receives a valid machine PAC from the end-user client, the machine identity details are extracted from the PAC and verified in the ACS external identity store. After these details are correctly verified, no further authentication is performed.</p> <p>Note ACS 5.8.1 only supports Active Directory as an external identity store for machine authentication.</p> <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 ACS 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> <ul style="list-style-type: none"> Enable Stateless Session Resume—Check for ACS to provision authorization PACs for EAP-FAST clients and always perform phase two of EAP-FAST (default = enabled). <p>Uncheck this option:</p> <ul style="list-style-type: none"> If you do not want ACS to provision authorization PACs for EAP-FAST clients. To always perform phase two of EAP-FAST. <p>When you check this option, you can enter the authorization period of the user authorization PAC. After this period the PAC expires. When ACS receives an expired authorization PAC, it performs phase two EAP-FAST authentication.</p>

Table 10-7 Access Service Properties—Allowed Protocols Page (continued)

Option	Description
Preferred EAP protocol	<p>Select the preferred EAP protocol from the following options available:</p> <ul style="list-style-type: none"> • EAP-FAST • PEAP • LEAP • EAP-TLS • EAP-MD5 <p>This option helps ACS to be flexible to work with old supplicants (end devices) which are not capable of sending No-Acknowledgment, when a particular protocol is not implemented. You can use this option to place a particular protocol first in list of protocols that is being negotiated with device so that the negotiation is successful.</p>
EAP-TLS L-bit	<p>Enables the L (length included) flag in access policies. When you perform EAP-TLS authentication against Terminal Wireless Local Area Network Unit (TWLU) client in ACS 5.x, the TWLU is expecting a L Flag (length included flag) set in change cipher specifications and the encrypted handshake message. If you are using the Honeywell TWLU unit, then it is recommended to create a group of all TWLU units and create an access policy with L flag included in it and use that access policy for all the TWLU units so that it will not disturb the other clients. The EAP-TLS L-bit is available at Access Policies > Access Services > Default Network Access > Edit: “Default Network Access” page in ACS web interface.</p>
Send as User-Name in RADIUS Access-Accept	
RADIUS Access-Request User-Name	Select this option if you want ACS to send the username that was received in the RADIUS access request in the RADIUS access accept response.
Principal User Name	Select this option if you want ACS to send the principal name of the certificate that is used to authenticate the user in the RADIUS access accept response.

- Step 3** Click **Finish** to save your changes to the access service.
- To enable an access service, you must add it to the service selection policy.

Configuring Access Services Templates

Use a service template to define an access service with policies that are customized to use specific condition types.

- Step 1** In the [Configuring General Access Service Properties, page 10-13](#), choose **Based on service template** and click **Select**.
- Step 2** Complete the fields as described in [Table 10-8](#):

Table 10-8 Access Services Templates

Template Name	Access Service Type	Protocols	Policies	Conditions	Results
Device Admin - Simple	Device Administration	PAP/ASCII	Identity	None - Simple	Internal users
			Authorization	Identity group, NDG:Location, NDG:Device Type, Time and Date	Shell profile
Device Admin - Command Auth	Device Administration	PAP/ASCII	Identity	None - Simple	Internal users
			Authorization	Identity group, NDG:Location, NDG: Time and Date	Command sets
Network Access - Simple	Network Access	PEAP, EAP-FAST	Identity	None - Simple	Internal users
			Authorization	NDG:Location, Time and date	Authorization profiles
Network Access - MAC Authentication Bypass	Network Access	Process Host Lookup, PAP/ASCII (detect PAP as host lookup) and EAP-MD5 (detect EAP-MD5 as host lookup)	Identity	None - Simple	Internal users
			Authorization	Use case	Authorization profiles

Deleting an Access Service

To delete an access service:

-
- Step 1** Select **Access Policies > Access Services**.
- The Access Services page appears with a list of configured services.
- Step 2** Check one or more check boxes the access services that you want to delete.
- Step 3** Click **Delete**; then click **OK** in the confirmation message.
- The Access Policies page appears without the deleted access service(s).
-

Related Topic

- [Creating, Duplicating, and Editing Access Services, page 10-12](#)

Configuring Access Service Policies

You configure access service policies after you create the access service:

- [Viewing Identity Policies, page 10-23](#)
- [Configuring Identity Policy Rule Properties, page 10-26](#)
- [Configuring a Group Mapping Policy, page 10-28](#)
- [Configuring a Session Authorization Policy for Network Access, page 10-31](#)
- [Configuring a Session Authorization Policy for Network Access, page 10-31](#)
- [Configuring Shell/Command Authorization Policies for Device Administration, page 10-36](#)

You can configure simple policies to apply to the same result to all incoming requests; or, you can create rule-based policies.

**Note**

If you create and save a simple policy, and then change to a rule-based policy, the simple policy becomes the default rule of the rule-based policy. If you have saved a rule-based policy and then change to a simple policy, you will lose all your rules except for the default rule. ACS automatically uses the default rule as the simple policy.

Before you begin to configure policy rules, you must:

- Configure the policy conditions and results. See [Managing Policy Conditions, page 9-1](#).
- Select the types of conditions and results that the policy rules apply. See [Customizing a Policy, page 10-4](#).

For information about configuring policy rules, see:

- [Creating Policy Rules, page 10-39](#)
- [Duplicating a Rule, page 10-40](#)
- [Editing Policy Rules, page 10-40](#)
- [Deleting Policy Rules, page 10-41](#)

Viewing Identity Policies

The identity policy in an access service defines the identity source that ACS uses for authentication and attribute retrieval. ACS can use the retrieved attributes in subsequent policies.

The identity source for:

- Password-based authentication can be a single identity store, or an identity store sequence.
- Certificate-based authentication can be a certificate authentication profile, or an identity store sequence.

An identity store sequence defines the sequence that is used for authentication and an optional additional sequence to retrieve attributes. See [Configuring Identity Store Sequences, page 8-101](#).

If you created an access service that includes an identity policy, you can configure and modify this policy. You can configure a simple policy, which applies the same identity source for authentication of all requests; or, you can configure a rule-based identity policy.

In the rule-based policy, each rule contains one or more conditions and a result, which is the identity source to use for authentication. You can create, duplicate, edit, and delete rules within the identity policy; and you can enable and disable them.

**Caution**

If you switch between the simple policy and the rule-based policy pages, you will lose your previously saved policy.

To configure a simple identity policy:

- Step 1** Select **Access Policies > Access Services > *service* > Identity**, where *service* is the name of the access service.

By default, the Simple Identity Policy page appears with the fields described in [Table 10-9](#):

Table 10-9 *Simple Identity Policy Page*

Option	Description
Policy type	<p>Defines the type of policy to configure:</p> <ul style="list-style-type: none"> Simple—Specifies the result to apply to all requests. Rule-based—Configure rules to apply different results, depending on the request. <p>If you switch between policy types, you will lose your previously saved policy configuration.</p>
Identity Source	<p>Identity source to apply to all requests. The default is Deny Access. For:</p> <ul style="list-style-type: none"> Password-based authentication, choose a single identity store, or an identity store sequence. Certificate-based authentication, choose a certificate authentication profile, or an identity store sequence. <p>The identity store sequence defines the sequence that is used for authentication and an optional additional sequence to retrieve attributes. See Configuring Identity Store Sequences, page 8-101.</p>
Advanced options	<p>Specifies whether to reject or drop the request, or continue with authentication for these options:</p> <ul style="list-style-type: none"> If authentication failed—Default is reject. If user not found—Default is reject. If process failed—Default is drop. <p>Owing to restrictions on the underlying protocol, ACS cannot always continue processing when the Continue option is chosen. ACS can continue when authentication fails for PAP/ASCII, EAP-TLS, or Host Lookup.</p> <p>For all other authentication protocols, the request will be dropped even if you choose the Continue option.</p>



- Step 2** Select an identity source for authentication; or, choose **Deny Access**.
- You can configure additional advanced options. See [Configuring Identity Policy Rule Properties, page 10-26](#).
- Step 3** Click **Save Changes** to save the policy.

Viewing Rules-Based Identity Policies

Select **Access Policies > Access Services > *service* > Identity**, where *<service>* is the name of the access service.

By default, the Simple Identity Policy page appears with the fields described in [Table 10-9](#). If configured, the Rules-Based Identity Policy page appears with the fields described in [Table 10-10](#):

Table 10-10 *Rule-based Identity Policy Page*

Option	Description
Policy type	<p>Defines the type of policy to configure:</p> <ul style="list-style-type: none"> Simple—Specifies the results to apply to all requests. Rule-based—Configure rules to apply different results depending on the request. <div>  Caution If you switch between policy types, you will lose your previously saved policy configuration. </div>
Status	<p>The current status of the rule. The rule statuses are:</p> <ul style="list-style-type: none"> Enabled—The rule is active. Disabled—ACS does not apply the results of the rule. Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The Monitor option is especially useful for watching the results of a new rule.
Name	Rule name.
Conditions	Conditions that determine the scope of the policy. This column displays all current conditions in subcolumns.
Results	Identity source that is used for authentication as a result of the evaluation of the rule.
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	<p>ACS applies the Default rule when:</p> <ul style="list-style-type: none"> Enabled rules are not matched. No other rules are defined. <p>Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.</p>
Customize button	<p>Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add.</p> <div>  Caution If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type. </div>
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10 .

To configure a rule-based policy, see these topics:

- [Creating Policy Rules, page 10-39](#)
- [Duplicating a Rule, page 10-40](#)
- [Editing Policy Rules, page 10-40](#)
- [Deleting Policy Rules, page 10-41](#)

For information about configuring an identity policy for Host Lookup requests, see [Configuring an Authorization Policy for Host Lookup Requests, page 4-19](#).

Related Topics

- [Configuring a Group Mapping Policy, page 10-28](#)
- [Configuring a Session Authorization Policy for Network Access, page 10-31](#)
- [Configuring a Session Authorization Policy for Network Access, page 10-31](#)
- [Configuring Shell/Command Authorization Policies for Device Administration, page 10-36](#)

Configuring Identity Policy Rule Properties

You can create, duplicate, or edit an identity policy rule to determine the identity databases that are used to authenticate the client and retrieve attributes for the client.

To display this page:

-
- Step 1** Choose **Access Policies > Access Services > service > Identity**, then do one of the following:
- **Click Create.**
 - Check a rule check box, and click **Duplicate**.
 - Click a rule name or check a rule check box, then click **Edit**.
- Step 2** Complete the fields as shown in the Identity Rule Properties page described in [Table 10-11](#):

Table 10-11 Identity Rule Properties Page

Option	Description
General	
Rule Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Rule Status	<p>Rule statuses are:</p> <ul style="list-style-type: none"> Enabled—The rule is active. Disabled—ACS does not apply the results of the rule. Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The Monitor option is especially useful for watching the results of a new rule.
Conditions	
conditions	<p>Conditions that you can configure for the rule. By default the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page.</p> <p>The default value for each condition is <i>ANY</i>. To change the value for a condition, check the condition check box, then specify the value.</p> <p>If you check Compound Condition, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-41.</p>
Results	
Identity Source	<p>Identity source to apply to requests. The default is Deny Access. For:</p> <ul style="list-style-type: none"> Password-based authentication, choose a single identity store, or an identity store sequence. Certificate-based authentication, choose a certificate authentication profile, or an identity store sequence. <p>The identity store sequence defines the sequence that is used for authentication and attribute retrieval and an optional sequence to retrieve additional attributes. See Configuring Identity Store Sequences, page 8-101.</p>
Advanced options	<p>Specifies whether to reject or drop the request, or continue with authentication for these options:</p> <ul style="list-style-type: none"> If authentication failed—Default is reject. If user not found—Default is reject. If process failed—Default is drop. <p>Owing to restrictions on the underlying protocol, ACS cannot always continue processing when the Continue option is chosen. ACS can continue when authentication fails for PAP/ASCII, EAP-TLS or Host Lookup.</p> <p>For all other authentication protocols, the request is dropped even if you choose the Continue option.</p>

Configuring a Group Mapping Policy

Configure a group mapping policy to map groups and attributes that are retrieved from external identity stores to ACS identity groups. When ACS processes a request for a user or host, this policy retrieves the relevant identity group which can be used in authorization policy rules.

If you created an access service that includes a group mapping policy, you can configure and modify this policy. You can configure a simple policy, which applies the same identity group to all requests; or, you can configure a rule-based policy.

In the rule-based policy, each rule contains one or more conditions and a result. The conditions can be based only on attributes or groups retrieved from external attribute stores, and the result is an identity group within the identity group hierarchy. You can create, duplicate, edit, and delete rules within the policy; and you can enable and disable them.

**Caution**

If you switch between the simple policy and the rule-based policy pages, you will lose your previously saved policy.

To configure a simple group mapping policy:

- Step 1** Select **Access Policies > Access Services > *service* > Group Mapping**, where *service* is the name of the access service.

By default, the Simple Group Mapping Policy page appears. See [Table 10-12](#) for field descriptions.

See [Table 10-13](#) for Rule-Based Group Mapping Policy page field descriptions.

Table 10-12 *Simple Group Mapping Policy Page*




Option	Description
Policy type	Defines the type of policy to configure: <ul style="list-style-type: none">Simple—Specifies the results to apply to all requests.Rule-based—Configure rules to apply different results depending on the request. <div>Caution If you switch between policy types, you will lose your previously saved policy configuration.</div>
Identity Group	Identity group to which attributes and groups from all requests are mapped.

Table 10-13 Rule-based Group Mapping Policy Page

Option	Description
Policy type	<p>Defines the type of policy to configure:</p> <ul style="list-style-type: none"> Simple—Specifies the results to apply to all requests. Rule-based—Configure rules to apply different results depending on the request. <p> Caution If you switch between policy types, you will lose your previously saved policy configuration.</p>
Status	<p>Current status of the rule. The rule statuses are:</p> <ul style="list-style-type: none"> Enabled—The rule is active. Disabled—ACS does not apply the results of the rule. Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	Rule name.
Conditions	Conditions that determine the scope of the policy. This column displays all current conditions in subcolumns.
Results	Identity group that is used as a result of the evaluation of the rule.
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	<p>ACS applies the Default rule when:</p> <ul style="list-style-type: none"> Enabled rules are not matched. No other rules are defined. <p>Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.</p>
Customize button	<p>Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add.</p> <p> Caution If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.</p>
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10 .

Step 2 Select an identity group.

Step 3 Click **Save Changes** to save the policy.

To configure a rule-based policy, see these topics:

- [Creating Policy Rules, page 10-39](#)
- [Duplicating a Rule, page 10-40](#)
- [Editing Policy Rules, page 10-40](#)

- [Deleting Policy Rules, page 10-41](#)

Related Topics

- [Viewing Identity Policies, page 10-23](#)
- [Configuring a Session Authorization Policy for Network Access, page 10-31](#)
- [Configuring a Session Authorization Policy for Network Access, page 10-31](#)
- [Configuring Shell/Command Authorization Policies for Device Administration, page 10-36](#)

Configuring Group Mapping Policy Rule Properties

Use this page to create, duplicate, or edit a group mapping policy rule to define the mapping of attributes and groups that are retrieved from external databases to ACS identity groups.

- Step 1** Select **Access Policies > Access Services > service > Group Mapping**, then do one of the following:
- Click **Create**.
 - Check a rule check box, and click **Duplicate**.
 - Click a rule name or check a rule check box, then click **Edit**.
- Step 2** Complete the fields as described in [Table 10-14](#):

Table 10-14 *Group Mapping Rule Properties Page*

Option	Description
General	
Rule Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Rule Status	Rule statuses are: <ul style="list-style-type: none"> • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Conditions	
conditions	<p>Conditions that you can configure for the rule. By default, the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page.</p> <p>The default value for each condition is ANY. To change the value for a condition, check the condition check box, then specify the value.</p> <p>If you check Compound Condition, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-41.</p>
Results	
Identity Group	Identity group to which attributes and groups from requests are mapped.

Configuring a Session Authorization Policy for Network Access

When you create an access service for network access authorization, it creates a Session Authorization policy. You can then add and modify rules to this policy to determine the access permissions for the client session.

You can create a standalone authorization policy for an access service, which is a standard first-match rule table. You can also create an authorization policy with an exception policy. See [Configuring Authorization Exception Policies, page 10-37](#). When a request matches an exception rule, the policy exception rule result is always applied.

The rules can contain any conditions and multiple results:

- Authorization profile—Defines the user-defined attributes and, optionally, the downloadable ACL that the Access-Accept message should return.
- Security Group Tag (SGT)—If you have installed Cisco Security Group Access, the authorization rules can define which SGT to apply to the request.

For information about how ACS processes rules with multiple authorization profiles, see [Processing Rules with Multiple Authorization Profiles, page 3-16](#).

To configure an authorization policy, see these topics:

- [Creating Policy Rules, page 10-39](#)
- [Duplicating a Rule, page 10-40](#)
- [Editing Policy Rules, page 10-40](#)
- [Deleting Policy Rules, page 10-41](#)


For information about creating an authorization policy for:

- Host Lookup requests, see [ACS and Cisco Security Group Access, page 4-22](#).
- Security Group Access support, see [Creating an Endpoint Admission Control Policy, page 4-25](#).

Step 1 Select **Access Policies > Access Services > *service* > Authorization**.

Step 2 Complete the fields as described in [Table 10-15](#):

Table 10-15 Network Access Authorization Policy Page

Option	Description
Status	<p>Rule statuses are:</p> <ul style="list-style-type: none"> Enabled—The rule is active. Disabled—ACS does not apply the results of the rule. Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	Name of the rule.
Conditions	
Identity Group	Name of the internal identity group to which this is matching against.
NDG:name	Network device group. The two predefined NDGs are Location and Device Type.
conditions	Conditions that define the scope of the rule. To change the types of conditions that the rule uses, click the Customize button. You must have previously defined the conditions that you want to use.
Results	
Authorization Profile	<p>Displays the authorization profile that will be applied when the corresponding rule is matched.</p> <p>When you enable the Security Group Access feature, you can customize rule results; a rule can determine the access permission of an endpoint, the security group of that endpoint, or both. The columns that appear reflect the customization settings.</p>
Hit Count	The number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	<p>ACS applies the Default rule when:</p> <ul style="list-style-type: none"> Enabled rules are not matched. No other rules are defined. <p>Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.</p>
Customize button	<p>Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add.</p> <p>When you enable the Security Group Access feature, you can also choose the set of rule results; only session authorization profiles, only security groups, or both.</p> <div>  <p>Caution If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.</p> </div>
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10 .

Configuring Network Access Authorization Rule Properties

Use this page to create, duplicate, and edit the rules to determine access permissions in a network access service.

Step 1 Select **Access Policies > Access Services > <service> > Authorization**, and click **Create, Edit, or Duplicate**.

Step 2 Complete the fields as described in [Table 10-16](#):

Table 10-16 Network Access Authorization Rule Properties Page

Option	Description
General	
Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Status	Rule statuses are: <ul style="list-style-type: none"> Enabled—The rule is active. Disabled—ACS does not apply the results of the rule. Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Conditions	
conditions	<p>Conditions that you can configure for the rule. By default the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page.</p> <p>The default value for each condition is ANY. To change the value for a condition, check the condition check box, then specify the value.</p> <p>If you check Compound Condition, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-41.</p>
Results	
Authorization Profiles	List of available and selected profiles. You can choose multiple authorization profiles to apply to a request. See Processing Rules with Multiple Authorization Profiles, page 3-16 for information about the importance of authorization profile order when resolving conflicts.
Security Group	<p>(Security Group Access only) The security group to apply.</p> <p>When you enable Security Group Access, you can customize the results options to display only session authorization profiles, only security groups, or both.</p>



Note

ACS allows you to create an internal user account using the identity string attribute to match a particular NDG:location only by configuring the detailed path of the NDG.

Configuring Device Administration Authorization Policies

A device administration authorization policy determines the authorizations and permissions for network administrators.

You create an authorization policy during access service creation. See [Configuring General Access Service Properties, page 10-13](#) for details of the Access Service Create page.


Use this page to:

- View rules.
- Delete rules.
- Open pages that enable you to create, duplicate, edit, and customize rules.

Select **Access Policies > Access Services > service > Authorization**.

The Device Administration Authorization Policy page appears as described in [Table 10-17](#).

Table 10-17 *Device Administration Authorization Policy Page*

Option	Description
Status	Rule statuses are: <ul style="list-style-type: none"> • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	Name of the rule.
Conditions	Conditions that define the scope of the rule. To change the types of conditions that the rule uses, click the Customize button. You must have previously defined the conditions that you want to use.
Results	Displays the shell profiles and command sets that will be applied when the corresponding rule is matched. You can customize rule results; a rule can apply shell profiles, or command sets, or both. The columns that appear reflect the customization settings.
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	ACS applies the Default rule when: <ul style="list-style-type: none"> • Enabled rules are not matched. • No other rules are defined. Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.
Customize button	Opens the Customize page in which you choose the types of conditions and results to use in policy rules. The Conditions and Results columns reflect your customized settings. <div>  <p>Caution If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.</p> </div>
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10 .

Configuring Device Administration Authorization Rule Properties

Use this page to create, duplicate, and edit the rules to determine authorizations and permissions in a device administration access service.

Select **Access Policies > Access Services > service > Authorization**, and click **Create**, **Edit**, or **Duplicate**.

The Device Administration Authorization Rule Properties page appears as described in [Table 10-18](#).

Table 10-18 *Device Administration Authorization Rule Properties Page*

Option	Description
General	
Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Status	Rule statuses are: <ul style="list-style-type: none"> • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Conditions	
conditions	<p>Conditions that you can configure for the rule. By default the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page.</p> <p>The default value for each condition is ANY. To change the value for a condition, check the condition check box, then specify the value.</p> <p>If you check Compound Condition, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-41.</p>
Results	
Shell Profiles	Shell profile to apply for the rule.
Command Sets	List of available and selected command sets. You can choose multiple command sets to apply.

Configuring Device Administration Authorization Exception Policies

You can create a device administration authorization exception policy for a defined authorization policy. Results from the exception rules always override authorization policy rules.


Use this page to:

- View exception rules.
- Delete exception rules.
- Open pages that create, duplicate, edit, and customize exception rules.

Select **Access Policies > Access Services > service > Authorization**, and click **Device Administration Authorization Exception Policy**.

The Device Administration Authorization Exception Policy page appears as described in [Table 10-19](#).

Table 10-19 Device Administration Authorization Exception Policy Page

Option	Description
Status	Rule statuses are: <ul style="list-style-type: none"> Enabled—The rule is active. Disabled—ACS does not apply the results of the rule. Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	Name of the rule.
Conditions	
Identity Group	Name of the internal identity group to which this is matching against.
NDG:name	Network device group. The two predefined NDGs are Location and Device Type.
Condition	Conditions that define the scope of the rule. To change the types of conditions that the rule uses, click the Customize button. You must have previously defined the conditions that you want to use.
Results	Displays the shell profile and command sets that will be applied when the corresponding rule is matched. You can customize rule results; a rule can determine the shell profile, the command sets, or both. The columns that appear reflect the customization settings.
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Customize button	Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. You do not need to use the same set of conditions and results as in the corresponding authorization policy. <div style="text-align: center;">  </div> Caution If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10 .

Configuring Shell/Command Authorization Policies for Device Administration

When you create an access service and select a service policy structure for Device Administration, ACS automatically creates a shell/command authorization policy. You can then create and modify policy rules.

The web interface supports the creation of multiple command sets for device administration. With this capability, you can maintain a smaller number of basic command sets. You can then choose the command sets in combination as rule results, rather than maintaining all the combinations themselves in individual command sets.

You can also create an authorization policy with an exception policy, which can override the standard policy results. See [Configuring Authorization Exception Policies, page 10-37](#).

For information about how ACS processes rules with multiple command sets, see [Processing Rules with Multiple Command Sets, page 3-11](#).

To configure rules, see:

- [Creating Policy Rules, page 10-39](#)
- [Duplicating a Rule, page 10-40](#)
- [Editing Policy Rules, page 10-40](#)
- [Deleting Policy Rules, page 10-41](#)

Configuring Authorization Exception Policies

An authorization policy can include exception policies. In general, exceptions are temporary policies; for example, to grant provisional access to visitors or increase the level of access to specific users. Use exception policies to react efficiently to changing circumstances and events.


The results from the exception rules always override the standard authorization policy rules.

You create exception policies in a separate rule table from the main authorization policy table. You do not need to use the same policy conditions in the exception policy as you used in the corresponding standard authorization policy.

To access the exception policy rules page:

-
- Step 1** Select **Access Policies > Service Selection Policy *service* > *authorization policy***, where *service* is the name of the access service, and *authorization policy* is the session authorization or shell/command set authorization policy.
- Step 2** In the Rule-Based Policy page, click the **Exception Policy** link above the rules table.
- The Exception Policy table appears with the fields described in [Table 10-20](#):

Table 10-20 Network Access Authorization Exception Policy Page

Option	Description
Status	<p>Rule statuses are:</p> <ul style="list-style-type: none"> Enabled—The rule is active. Disabled—ACS does not apply the results of the rule. Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	Name of the rule.
Conditions	
Identity Group	Name of the internal identity group to which this is matching against.
NDG:name	Network device group. The two predefined NDGs are Location and Device Type.
Condition Name	Conditions that define the scope of the rule. To change the types of conditions that the rule uses, click the Customize button. You must have previously defined the conditions that you want to use.
Results	<p>Displays the authorization profile that will be applied when the corresponding rule is matched.</p> <p>When you enable the Security Group Access feature, you can customize rule results; a rule can determine the access permission of an endpoint, the security group of that endpoint, or both. The columns that appear reflect the customization settings.</p>
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Customize button	<p>Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. You do not need to use the same set of conditions as in the corresponding authorization policy.</p> <p>When you enable the Security Group Access feature, you can also choose the set of rule results; only session authorization profiles, only security groups, or both.</p> <div>  <p>Caution If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.</p> </div>
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10 .

To configure rules, see:

- [Creating Policy Rules, page 10-39](#)
- [Duplicating a Rule, page 10-40](#)
- [Editing Policy Rules, page 10-40](#)
- [Deleting Policy Rules, page 10-41](#)

Related Topics

- [Configuring a Session Authorization Policy for Network Access, page 10-31](#)
- [Configuring Shell/Command Authorization Policies for Device Administration, page 10-36](#)

Creating Policy Rules

When you create rules, remember that the order of the rules is important. When ACS encounters a match as it processes the request of a client that tries to access the ACS network, all further processing stops and the associated result of that match is found. No further rules are considered after a match is found.

The Default Rule provides a default policy in cases where no rules are matched or defined. You can edit the result of a default rule.

Before You Begin

- Configure the policy conditions and results. See [Managing Policy Conditions, page 9-1](#).
- Select the types of conditions and results that the policy rules apply. See [Customizing a Policy, page 10-4](#).

To create a new policy rule:

-
- Step 1** Select **Access Policies > Service Selection Policy *service* > *policy***, where *service* is the name of the access service, and *policy* is the type of policy. If you:
- Previously created a rule-based policy, the Rule-Based Policy page appears, with a list of configured rules.
 - Have not created a rule-based policy, the Simple Policy page appears. Click **Rule-Based**.
- Step 2** In the Rule-Based Policy page, click **Create**.
- The Rule page appears.
- Step 3** Define the rule.
- Step 4** Click **OK**
- The Policy page appears with the new rule.
- Step 5** Click **Save Changes** to save the new rule.
-

To configure a simple policy to use the same result for all requests that an access service processes, see:

- [Viewing Identity Policies, page 10-23](#)
- [Configuring a Group Mapping Policy, page 10-28](#)
- [Configuring a Session Authorization Policy for Network Access, page 10-31](#)
- [Configuring a Session Authorization Policy for Network Access, page 10-31](#)
- [Configuring Shell/Command Authorization Policies for Device Administration, page 10-36](#)

Related Topics

- [Duplicating a Rule, page 10-40](#)
- [Editing Policy Rules, page 10-40](#)
- [Deleting Policy Rules, page 10-41](#)



Note

ACS 5.8.1 displays a detailed audit reports on ACS configuration audit reports page for creating, editing, or re-ordering access service policies from the ACS web interface.

Duplicating a Rule

You can duplicate a rule if you want to create a new rule that is the same, or very similar to, an existing rule. The duplicate rule name is based on the original rule with parentheses to indicate duplication; for example, Rule-1(1).

After duplication is complete, you access each rule (original and duplicated) separately.

**Note**

You cannot duplicate the Default rule.

To duplicate a rule:

-
- Step 1** Select **Access Policies > Service Selection Policy > *service* > *policy***, where *service* is the name of the access service, and *policy* is the type of policy.
The Policy page appears with a list of configured rules.
 - Step 2** Check the check box the rule that you want to duplicate. You cannot duplicate the Default Rule.
 - Step 3** Click **Duplicate**.
The Rule page appears.
 - Step 4** Change the name of the rule and complete the other applicable field options.
 - Step 5** Click **OK**.
The Policy page appears with the new rule.
 - Step 6** Click **Save Changes** to save the new rule.
 - Step 7** Click **Discard Changes** to cancel the duplicate rule.
-

Related Topics

- [Creating Policy Rules, page 10-39](#)
- [Editing Policy Rules, page 10-40](#)
- [Deleting Policy Rules, page 10-41](#)

Editing Policy Rules

You can edit all values of policy rules; you can also edit the result in the Default rule.

To edit a rule:

-
- Step 1** Select **Access Policies > Service Selection Policy > *service* > *policy***, where *service* is the name of the access service, and *policy* is the type of policy.
The Policy page appears, with a list of configured rules.
 - Step 2** Click the rule name that you want to modify; or, check the check box for the Name and click **Edit**.
The Rule page appears.
 - Step 3** Edit the appropriate values.
 - Step 4** Click **OK**.

The Policy page appears with the edited rule.

Step 5 Click **Save Changes** to save the new configuration.

Step 6 Click **Discard Changes** to cancel the edited information.

Related Topics

- [Creating Policy Rules, page 10-39](#)
- [Duplicating a Rule, page 10-40](#)
- [Deleting Policy Rules, page 10-41](#)

Deleting Policy Rules



Note You cannot delete the Default rule.

To delete a policy rule:

Step 1 Select **Access Policies > Service Selection Policy > *service* > *policy***, where *service* is the name of the access service, and *policy* is the type of policy.

The Policy page appears, with a list of configured rules.

Step 2 Check one or more check boxes the rules that you want to delete.

Step 3 Click **Delete**.

The Policy page appears without the deleted rule(s).

Step 4 Click **Save Changes** to save the new configuration.

Step 5 Click **Discard Changes** to retain the deleted information.

Related Topics

- [Creating Policy Rules, page 10-39](#)
- [Duplicating a Rule, page 10-40](#)
- [Editing Policy Rules, page 10-40](#)

Configuring Compound Conditions

Use compound conditions to define a set of conditions based on any attributes allowed in simple policy conditions. You define compound conditions in a policy rule page; you cannot define them as separate condition objects.

This section contains the following topics:

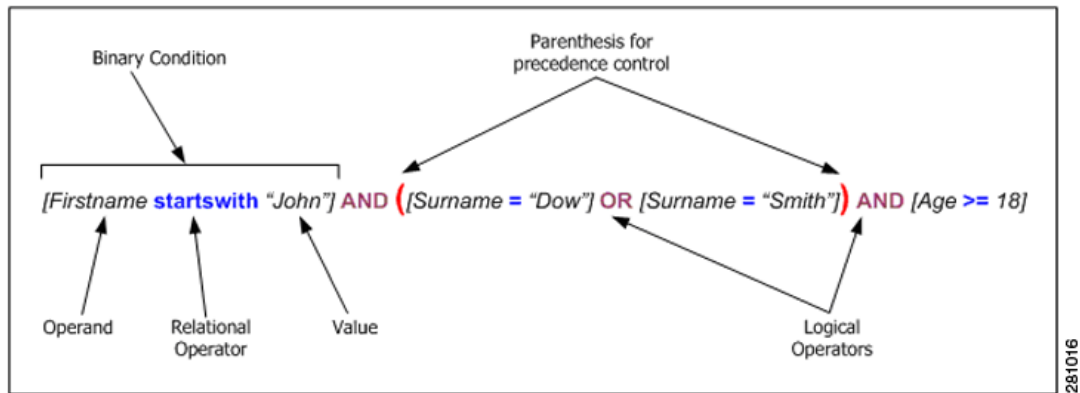
- [Compound Condition Building Blocks, page 10-42](#)
- [Types of Compound Conditions, page 10-43](#)

- [Using the Compound Expression Builder, page 10-46](#)

Compound Condition Building Blocks

Figure 10-1 shows the building blocks of a compound condition.

Figure 10-1 Building Blocks of a Compound Condition



- **Operands**—Any attribute or condition type, such as Protocol/Request Attributes, Identity Attributes, Identity Groups, Network Device Groups (NDGs), Date/Time, and Custom or Standard Conditions.
- **Relational Operators**—Operators that specify the relation between an operand and a value; for example, equals (=), or does not match. The operators that you can use in any condition vary according to the type of operand.
- **Binary condition**—A binary condition defines the relation between a specified operand and value; for example, [username = "Smith"].
- **Logical Operators**—The logical operators operate on or between binary conditions. The supported logical operators are AND and OR.
- **Precedence Control**—You can alter the precedence of logical operators by using parentheses. Nested parentheses provide administrator control of precedence. The natural precedence of logical operators, that is, without parenthesis intervention, is NOT, AND, OR, where NOT has the highest precedence and OR the lowest.

Table 10-21 summarizes the supported dynamic attribute mapping while building Compound Conditions.

Table 10-21 Supported Dynamic Attribute Mapping in Policy Compound Condition

Operand1	Operand2	Example
String attribute	String attribute	—
Integer attribute	Integer attribute	—
Enumeration attribute	Enumeration attribute	—
Boolean attribute	Boolean attribute	—
IP address attribute	IP address attribute	—
Special cases		

Table 10-21 Supported Dynamic Attribute Mapping in Policy Compound Condition

Operand1	Operand2	Example
Hierarchical attribute	String attribute	NDG:Customer vs. 'Internal Users' string attribute
String attribute	Hierarchical attribute	—

**Note**

Dynamic attribute mapping is not applicable for ExternalGroups attribute of Type "String Enum" and "Time And Date" attribute of type "Date Time Period".

For hierarchical attribute, the value is appended with attribute name so while configuring any string attribute to compare with hierarchical attribute the value of the string attribute has to start with hierarchical attribute name.

For example:

- When you define a new string attribute named *UrsAttr* to compare against *DeviceGroup* attribute created under NDG, then the value of the *UrsAttr* has to be configured as follows:
DeviceGroup: *Value*
- When you want to compare a string attribute with *UserIdentityGroup* which is a hierarchy type attribute within each internal users, then the string attribute has to be configured as follows:
IdentityGroup:All Groups:"Identity Group Name"

Related Topics

- [Types of Compound Conditions, page 10-43](#)
- [Using the Compound Expression Builder, page 10-46](#)

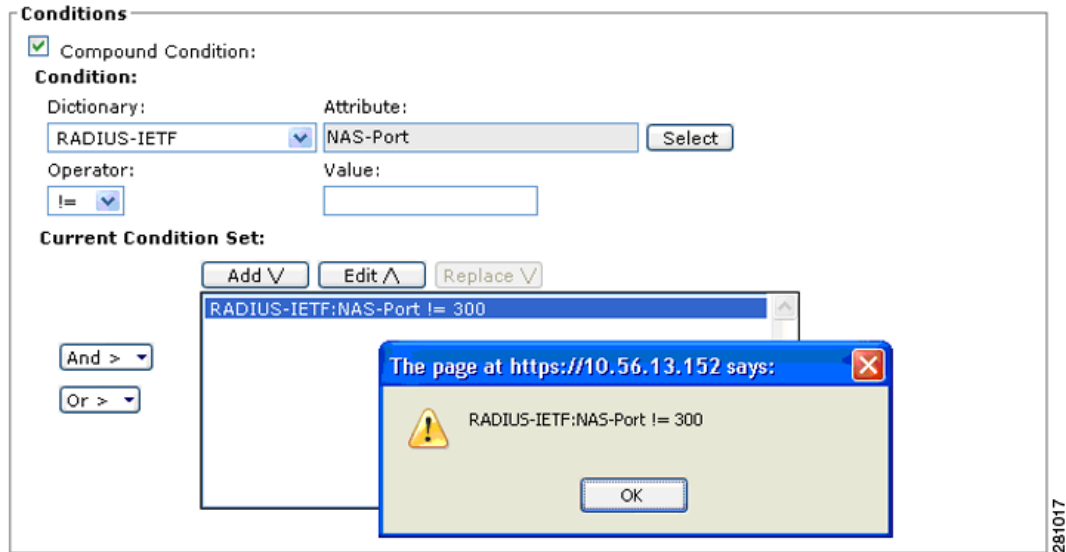
Types of Compound Conditions

You can create three types of compound conditions:

Atomic Condition

Consists of a single predicate and is the only entry in the list. Because all simple conditions in a rule table, except for NDGs, assume the equals (=) operation between the attribute and value, the atomic condition is used to choose an operator other than equals (=). See [Figure 10-2](#) for an example.

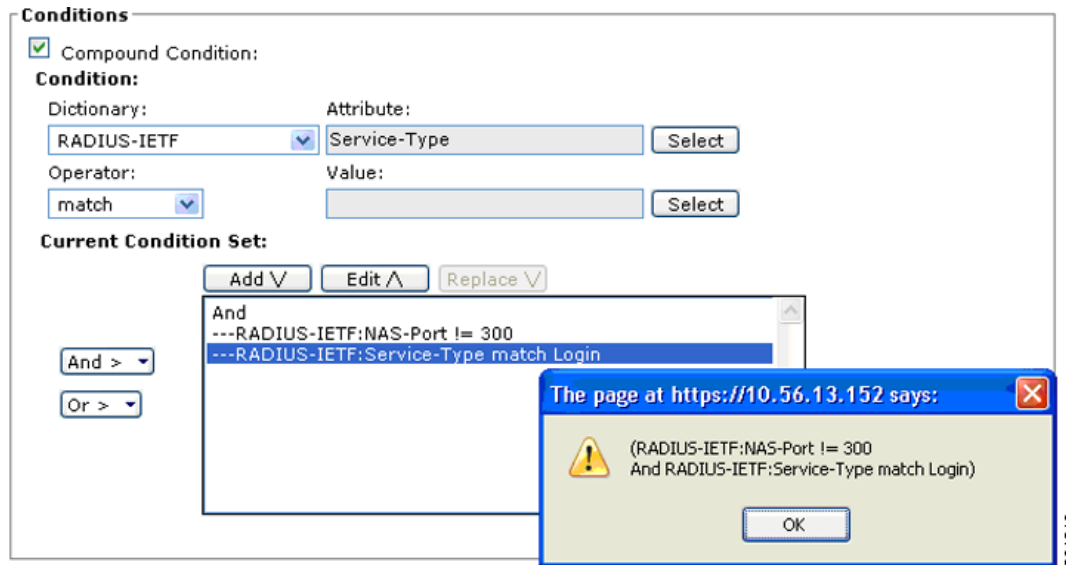
Figure 10-2 Compound Expression - Atomic Condition



Single Nested Compound Condition

Consists of a single operator followed by a set of predicates (≥ 2). The operator is applied between each of the predicates. See Figure 10-3 for an example. The preview window displays parentheses $()$ to indicate precedence of logical operators.

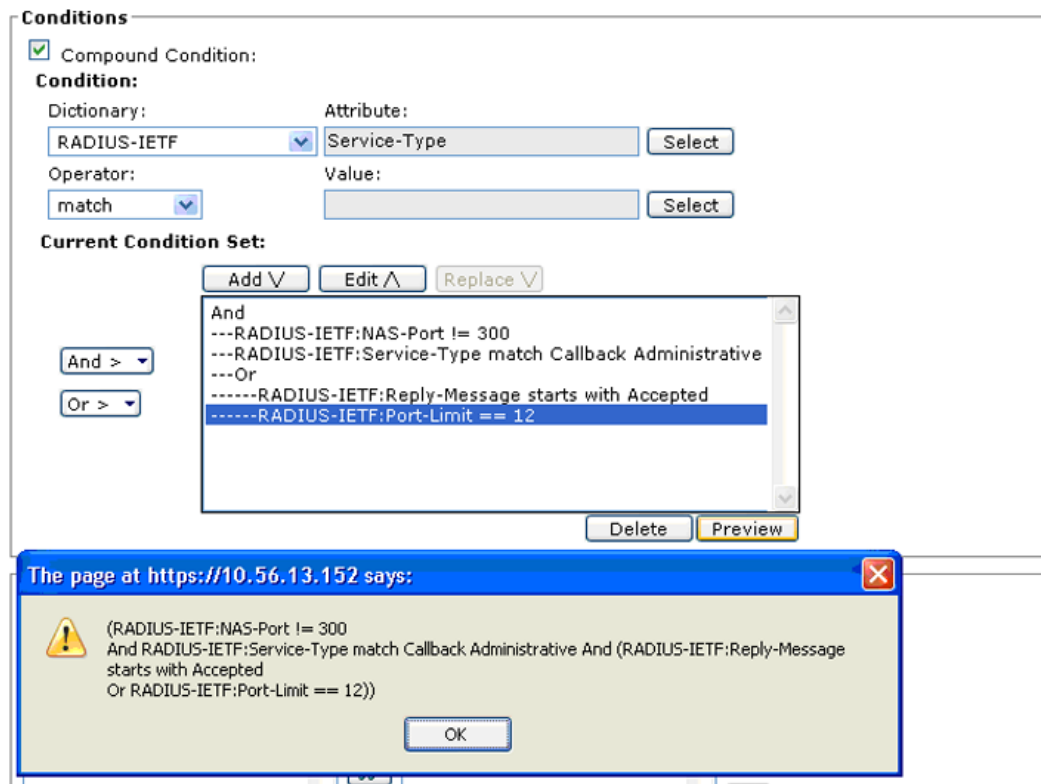
Figure 10-3 Single Nested Compound Expression



Multiple Nested Compound Condition

You can extend the simple nested compound condition by replacing any predicate in the condition with another simple nested compound condition. See Figure 10-4 for an example. The preview window displays parentheses $()$ to indicate precedence of logical operators.

Figure 10-4 Multiple Nested Compound Expression

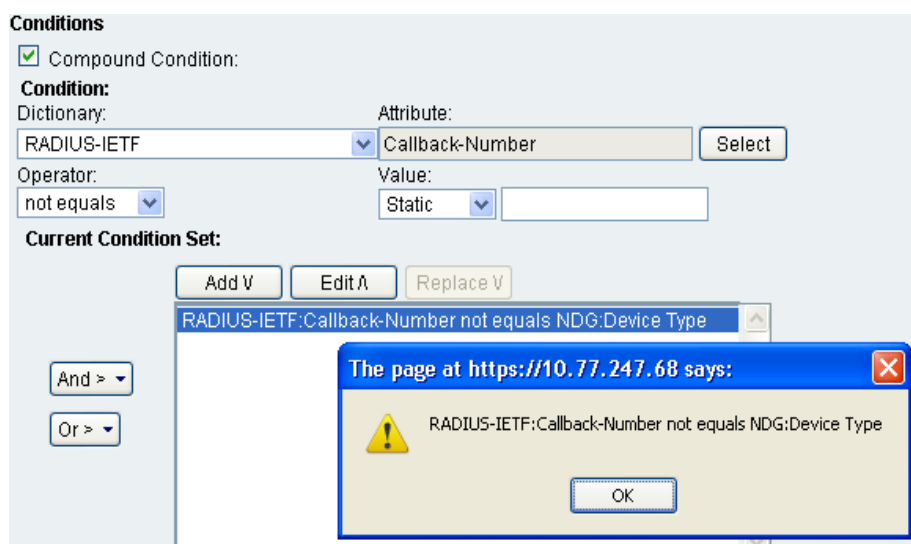


281019

Compound Expression with Dynamic value

You can select dynamic value to select another dictionary attribute to compare against the dictionary attribute selected as operand. See Figure 10-5 for an example.

Figure 10-5 Compound Expression Builder with Dynamic Value



282674

Related Topics

- [Compound Condition Building Blocks, page 10-42](#)
- [Using the Compound Expression Builder, page 10-46](#)

Using the Compound Expression Builder

You construct compound conditions by using the expression builder in Rule Properties pages. The expression builder contains two sections: a predicate builder to create primary conditions and controls for managing the expression.

In the first section, you define the primary conditions. Choose the dictionary and attribute to define the operand, then choose the operator, and specify a value for the condition. Use the second section to organize the order of conditions and the logical operators that operate on or between binary conditions.

[Table 10-22](#) describes the fields in the compound expression builder.

Table 10-22 *Expression Builder Fields*

Field	Description
Condition	Use this section to define the primary conditions.
Dictionary	Specifies the dictionary from which to take the operand. These available options depend on the policy that you are defining. For example, when you define a service selection policy, the Identity dictionaries are not available.
Attribute	Specifies the attribute that is the operand of the condition. The available attributes depend on the dictionary that you chose.
Operator	The relational operator content is dynamically determined according to the choice in the preceding operand field.
Value	The condition value. The type of this field depends on the type of condition or attribute. Select one of the following two options: <ul style="list-style-type: none"> • Static—If selected, you have to enter or select the static value depending on attribute type. • Dynamic—If selected, you can select another dictionary attribute to compare against the dictionary attribute selected as operand.
Current Condition Set	Use this section to organize the order of conditions and the logical operators that operate on or between binary conditions.
Condition list	Displays a list of defined binary conditions for the compound conditions and their associated logical operators.
Add	After you define a binary condition, click Add to add it to the Condition list.
Edit	To edit a binary condition, select the condition in the Condition list and click Edit. The condition properties appear in the Condition fields. Modify the condition as required, then click Replace.
Replace	Click to replace the selected condition with the condition currently defined in the Condition fields.
And Or	Specifies the logical operator on a selected condition, or between the selected condition and the one above it. Click the appropriate operator, and click Insert to add the operator as a separate line; click the operator and click Replace, to replace the selected line.
Delete	Click to delete the selected binary condition or operator from the condition list.
Preview	Click to display the current expression in corresponding parenthesis representation. The rule table displays the parenthesis representation after the compound expression is created.

Related Topics

- [Compound Condition Building Blocks, page 10-42](#)
- [Types of Compound Conditions, page 10-43](#)

Security Group Access Control Pages

This section contains the following topics:

- [Egress Policy Matrix Page, page 10-47](#)
- [Editing a Cell in the Egress Policy Matrix, page 10-48](#)
- [Defining a Default Policy for Egress Policy Page, page 10-48](#)
- [NDAC Policy Page, page 10-49](#)
- [NDAC Policy Properties Page, page 10-50](#)
- [Network Device Access EAP-FAST Settings Page, page 10-51](#)

Egress Policy Matrix Page

The Egress policy, also known as an SGACL policy, determines which SGACLs to apply at the Egress points of the network, based on the source and destination SGTs. ACS presents the Egress policy as a matrix; it displays all the security groups in the source and destination axes. Each cell in the matrix can contain a set of ACLs to apply to the corresponding source and destination SGTs.

The network devices add the default policy to the specific policies that you defined for the cells. For empty cells, only the default policy applies.

Use the Egress policy matrix to view, define, and edit the sets of ACLs to apply to the corresponding source and destination SGTs.

To display this page, choose **Access Policies > Security Group Access Control > Egress Policy**.

Table 10-23 *Egress Policy Matrix Page*

Option	Description
Destination Security Group	Column header displaying all destination security groups.
Source Security Group	Row header displaying all source security groups.
Cells	Contain the SGACLs to apply to the corresponding source and destination security group.
Edit	Click a cell, then click Edit to open the Edit dialog box for that cell. See Editing a Cell in the Egress Policy Matrix, page 10-48 .
Default Policy	Click to open a dialog box to define the default Egress policy. See Defining a Default Policy for Egress Policy Page, page 10-48 .
Set Matrix View	To change the Egress policy matrix display, choose an option, then click Go : <ul style="list-style-type: none"> • All—Clears all the rows and columns in the Egress policy matrix. • Customize View—Launches a window where you can customize source and destination security groups corresponding to the selected cell.

Related Topic

- [Creating an Egress Policy, page 4-26](#)

Editing a Cell in the Egress Policy Matrix

Use this page to configure the policy for the selected cell. You can configure the SGACLs to apply to the corresponding source and destination security group.

To display this page, choose **Access Policies > Security Group Access Control > Egress Policy**, select a cell, then click **Edit**.

Table 10-24 *Edit Cell Page*

Option	Description
Configure Security Groups	<i>Display only.</i> Displays the source and destination security group name for the selected cell.
General	Description for the cell policy.
ACLs	Move the SGACLs that you want to apply to the corresponding source and destination security group from the Available list to the Selected list. To specify the order of the list of SGACLs, use the Up (^) and Down (v) arrows.

Related Topic

- [Creating an Egress Policy, page 4-26](#)

Defining a Default Policy for Egress Policy Page

Use this page to define the default Egress policy. The network devices add the default policy to the specific policies defined for the cells. For empty cells, only the default policy applies.

To display this page, choose **Access Policies > Security Group Access Control > Egress Policy**, then click **Default Policy**.

Table 10-25 *Default Policy Page*

Option	Description
ACLs	Move the SGACLs that you want to apply to the corresponding source and destination security group from the Available list to the Selected list. To specify the order of the list of SGACLs, use the Up (^) and Down (v) arrows. Select Permit All or Deny All as a final catch-all rule.

Related Topics

- [Creating an Egress Policy, page 4-26](#)
- [Creating a Default Policy, page 4-27](#)

NDAC Policy Page

The Network Device Admission Control (NDAC) policy determines the SGT for network devices in a Security Group Access environment. The NDAC policy handles:

- Peer authorization requests from one device about its neighbor.
- Environment requests (a device is collecting information about itself).

The policy returns the same SGT for a specific device, regardless of the request type.



Note

You do not add an NDAC policy to an access service; it is implemented by default. However, for endpoint admission control, you must define an access service and session authorization policy. See [Configuring Network Access Authorization Rule Properties, page 10-33](#), for information about creating a session authorization policy.

Use this page to configure a simple policy that assigns the same security group to all devices, or configure a rule-based policy.

To display this page, choose **Access Policies > Security Group Access Control > Network Device Access > Authentication Policy**.

If you have already configured an NDAC policy, the corresponding Simple Policy page or Rule-based Policy page opens; otherwise, the Simple Policy page opens by default.

Simple Policy Page

Use this page to define a simple NDAC policy.

Table 10-26 *Simple NDAC Policy Page*


Option	Description
Policy type	<p>Defines the type of policy to configure:</p> <ul style="list-style-type: none"> • Simple—Specifies that the result applies to all requests. • Rule-based—Configure rules to apply different results depending on the request. <p>If you switch between policy types, you will lose your previously saved policy configuration.</p>
Security Group	Select the security group to assign to devices. The default is Unknown.

Rule-Based Policy Page

Use this page for a rule-based policy to:

- View rules.
- Delete rules.
- Open pages that create, duplicate, edit, and customize rules.

Table 10-27 Rule-Based NDAC Policy Page

Option	Description
Policy type	<p>Defines the type of policy to configure:</p> <ul style="list-style-type: none"> Simple—Specifies the result to apply to all requests. Rule-based—Configure rules to apply different results depending on the request. <p>If you switch between policy types, you will lose your previously saved policy configuration.</p>
Status	<p>Rule statuses are:</p> <ul style="list-style-type: none"> Enabled—The rule is active. Disabled—ACS does not apply the results of the rule. Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Name	<p>Name of the rule. The Default Rule is available for conditions for which:</p> <ul style="list-style-type: none"> Enabled rules are not matched. Rules are not defined. <p>Click a link to edit or duplicate a rule.</p> <p>You can edit the Default Rule but you cannot delete, disable, or duplicate it.</p>
Conditions	Conditions that you can use to define policy rules. To change the display of rule conditions, click the Customize button. You must have previously defined the conditions that you want to use.
Results	Displays the security group assigned to the device when it matches the corresponding condition.
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Customize button	<p>Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add. You do not need to use the same set of conditions as in the corresponding authorization policy.</p> <p> Caution If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.</p>
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10 .

Related Topics:

- [Configuring an NDAC Policy, page 4-24](#)
- [NDAC Policy Properties Page, page 10-50](#)

NDAC Policy Properties Page

Use this page to create, duplicate, and edit rules to determine the SGT for a device.

To display this page, choose **Access Policies > Security Group Access Control > Network Device Access > Authentication Policy**, then click **Create**, **Edit**, or **Duplicate**.

**Note**

For endpoint admission control, you must define an access service and session authorization policy. See [Configuring Network Access Authorization Rule Properties, page 10-33](#) for information about creating a session authorization policy.

Table 10-28 *NDAC Policy Properties Page*

Option	Description
General	
Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Status	Rule statuses are: <ul style="list-style-type: none"> • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The monitor option is especially useful for watching the results of a new rule.
Conditions	
conditions	<p>Conditions that you can configure for the rule. The default value for each condition is ANY. To change the value for a condition, check the condition check box, then enter the value.</p> <p>If compound expression conditions are available, when you check Compound Expression, an expression builder appears. For more information, see Configuring Compound Conditions, page 10-41.</p> <p>To change the list of conditions for the policy, click the Customize button in the NDAC Policy Page, page 10-49.</p>
Results	
Security Group	Select the security group to assign to the device when it matches the corresponding conditions.

Related Topics:

- [Configuring an NDAC Policy, page 4-24](#)
- [NDAC Policy Page, page 10-49](#)

Network Device Access EAP-FAST Settings Page

Use this page to configure parameters for the EAP-FAST protocol that the NDAC policy uses.

To display this page, choose **Access Policies > Security Group Access Control > Network Device Access**.

Table 10-29 *Network Device Access EAP-FAST Settings Page*

Option	Description
EAP-FAST Settings	

Table 10-29 Network Device Access EAP-FAST Settings Page (continued)

Option	Description
Tunnel PAC Time To Live	Time to live (TTL), or duration, of a PAC before it expires and requires replacing.
Proactive PAC Update When % of PAC TTL is Left	Percentage of PAC TTL remaining when you should update the PAC.

Related Topics:

- [Configuring an NDAC Policy, page 4-24](#)
- [Configuring EAP-FAST Settings for Security Group Access, page 4-25](#)
- [NDAC Policy Page, page 10-49](#)

Maximum User Sessions

For optimal performance, you can limit the number of concurrent users accessing network resources. ACS 5.8.1 imposes limits on the number of concurrent service sessions per user.

The limits are set in several different ways. You can set the limits at the user level or at the group level. Depending upon the maximum user session configurations, the session count is applied to the user.

**Note**

To make the maximum sessions work for user access, the administrator should configure RADIUS accounting.

**Note**

To make the maximum sessions work for device management, the administrator should configure TACACS+ session authorization and accounting.

This section contains the following topics:

- [Maximum Session User Settings, page 10-52](#)
- [Maximum Session Group Settings, page 10-53](#)
- [Maximum Session Global Settings, page 10-55](#)
- [Purging User Sessions, page 10-55](#)
- [Maximum User Session in Distributed Environment, page 10-56](#)
- [Maximum User Session in Proxy Scenario, page 10-57](#)

Maximum Session User Settings

You can configure maximum user sessions for each user globally.

To configure maximum user sessions:

-
- Step 1** Choose **Access Policies > Max User Session Policy > Max Session User Settings**.
- Step 2** Specify a **Max User Session Value**, for the maximum number of concurrent sessions permitted.

- Step 3** Check the **Unlimited Sessions** check box if you want users to have unlimited sessions.
- Step 4** Click **Submit**.

**Note**

If the maximum number of sessions is configured at both the user and group level, the smaller value will have precedence.

For example:

Given a user Bob in the group America:US:West with a maximum session value of 5 sessions for the group and a maximum session value of 10 for the user. In this case, user Bob can have a maximum of 5 sessions only.

Related Topics

- [Maximum Session Group Settings, page 10-53](#)
- [Maximum Session Global Settings, page 10-55](#)
- [Purging User Sessions, page 10-55](#)
- [Maximum User Session in Distributed Environment, page 10-56](#)
- [Maximum User Session in Proxy Scenario, page 10-57](#)

Maximum Session Group Settings

You can configure the maximum number of sessions for the identity groups. All the sessions can sometimes be used by a few users in the group. Requests from other users to create a new session are rejected because the number of sessions has already reached the maximum configured value.

ACS 5.8.1 allows you to configure a maximum session limit for any user in the group; for example, each user belonging to a specific Identity Group may open not more than the session limit, no matter how many sessions other users from the same group have opened. There is no option to set up a session limit for a particular user.

From the ACS web interface, you can configure the Maximum Sessions limit for a user belonging to an identity group from the ACS web interface.

The ACS 4.x migration utility includes migrating the maximum session configuration.

When calculating the session limit for a particular user, the lowest configuration value takes the precedence—whether the global session limit per user, the session limit per identity group that the user belongs to, or the session limit per user in the group.

To configure maximum sessions for a group:

- Step 1** Choose **Access Policies > Max User Session Policy > Max Session Group Settings**.
All the configured identity groups are listed.
- Step 2** Check the check box the group for which you want to configure a maximum number of sessions.
- Step 3** Click **Edit**.
- Step 4** Complete the fields as described in [Table 10-30](#).

Table 10-30 Max User Session Global Settings Page

Option	Description
General	
Name	Name of the Identity Group.
Description	Description of the Identity Group.
Max Session Group Settings	
Unlimited Session	Check this check box if you want to provide unlimited sessions to the group.
Max Session for Group	Specify a value for the maximum number of concurrent sessions permitted for the group.
Unlimited Sessions for Users in Group	Check this check box if you want to provide unlimited sessions for each user in a group.
Max Session for User in Group	Specify a value for the maximum number of concurrent sessions permitted for each user in a group. This option overrides the maximum number of sessions for a group.

Step 5 Click Submit.

Unlimited is selected by default. Group-level session limits are applied based on the hierarchy. For example:

The group hierarchy is *America:US:West:CA* and the maximum sessions are as follows:

- America: 100 max sessions
- US: 80 max sessions
- West: 75 max sessions
- CA: 50 max sessions

If “Max Session for User in Group X” is set to N, each user belonging to the group X may open not more than N sessions.

If the user belongs to *America/US/West*, ACS checks that the number of sessions does not exceed the limit that is specified for the parent groups *America/US/West*, *America/US*, *America*. When you set the maximum number of sessions of a user group to 100, the total count of all sessions established by all members of that group cannot exceed 100. Once the session is allowed, the Number of Active Sessions Availed counter for the three nodes is increased by one. The ACS runtime component takes care of this validation during authentication.

**Note**

If the maximum number of sessions is configured at the group level, at the user level within a group level, and at the user level globally, then ACS considers the least value among them.

Related Topics

- [Maximum Session User Settings, page 10-52](#)
- [Maximum Session Global Settings, page 10-55](#)
- [Purging User Sessions, page 10-55](#)
- [Maximum User Session in Distributed Environment, page 10-56](#)
- [Maximum User Session in Proxy Scenario, page 10-57](#)

Maximum Session Global Settings

You can assign session keys for RADIUS and TACACS+ requests. A session key is provided with a set of attributes for RADIUS and TACACS+. You can customize the session key attributes according to your environment. If you do not assign a session key, ACS uses the default session key values.

A session key is a unique key that is used to track user sessions. The session key helps ACS differentiate between a user re-authenticating to the same session and a user starting a new session. The session key attributes for a single session should be the same in the access request and in the accounting start packet. The Session key helps ACS to identify the session properly. When ACS re-authenticates the same session again, the same key is retained.

To configure the global settings for maximum user sessions, choose **System Administration > Users > Max User Session Global Settings**.

Table 10-31 Max User Session Global Settings Page

Option	Description
RADIUS Session Key Assignment	
Available Session Keys	RADIUS sessions keys available for assignment. Note To use the RADIUS Acct-Session-Id (attribute #44) in the RADIUS session key, you should configure the Acct-Session-Id to be sent in the access request: <code>Router(config)# radius-server attribute 44 include-in-access-req</code>
Assigned Session Keys	RADIUS session key assigned. The default session keys for RADIUS are: UserName:NAS-Identifier:NAS-Port:Calling-Station-ID
TACACS+ Session Key Assignment	
Available Session Keys	TACACS+ sessions keys available for assignment.
Assigned Session Keys	TACACS+ session key that have been assigned. The default session keys for TACACS+ are: User:NAS-Address:Port:Remote-Address
Max User Session Timeout Settings	
Unlimited Session Timeout	No timeout.
Max User Session Timeout	Once the session timeout is reached, ACS sends a fake STOP packet to close the respective session and updates the session count. Note The user is not forced to log out of the device.

Related Topics

- [Maximum Session User Settings, page 10-52](#)
- [Maximum Session Group Settings, page 10-53](#)
- [Purging User Sessions, page 10-55](#)
- [Maximum User Session in Distributed Environment, page 10-56](#)
- [Maximum User Session in Proxy Scenario, page 10-57](#)

Purging User Sessions

You can use the Purge option only when users are listed as Logged-in but connection to the AAA client has been lost and the users are no longer actually logged in.

Purging will not log off the user from the AAA client, however it will decrease the session count by one. While the count is zero, any interim updates or STOP packet that arrives from the device will be discarded. Due to this purging, if a user logged in with the same user name and password in another AAA client, this session will not be affected.

**Note**

A fake accounting stop is sent irrespective of the session count value.

To purge the User session:

-
- Step 1** Go to **System Administration > Users > Purge User Sessions**.
- The Purge User Session page appears with a list of all AAA clients.
- Step 2** Select the AAA client for which you want to purge the user sessions.
- Step 3** Click **Get Logged-in User List**.
- A list of all the logged in users is displayed.
- Step 4** Click **Purge All Sessions** to purge all the user session logged in to the particular AAA client.
-

Related Topics

- [Maximum Session User Settings, page 10-52](#)
- [Maximum Session Group Settings, page 10-53](#)
- [Maximum Session Global Settings, page 10-55](#)
- [Maximum User Session in Distributed Environment, page 10-56](#)
- [Maximum User Session in Proxy Scenario, page 10-57](#)

Maximum User Session in Distributed Environment

In distributed environment, all the user and identity group configurations are replicated to the secondaries except the session cache related information with respect to maximum user session maintained by runtime. Hence, each server has its own session established details in the runtime. Also, the maximum session count gets applied based on which ACS server the authentication/accounting request is received on.

Related Topics

- [Maximum Session User Settings, page 10-52](#)
- [Maximum Session Group Settings, page 10-53](#)
- [Maximum Session Global Settings, page 10-55](#)
- [Purging User Sessions, page 10-55](#)
- [Maximum User Session in Proxy Scenario, page 10-57](#)

Maximum User Session in Proxy Scenario

Authentication and accounting requests should be sent to the same ACS server; else the Maximum Session feature will not work as desired.

Related Topics

- [Maximum User Sessions, page 10-52](#)
- [Maximum Session User Settings, page 10-52](#)
- [Maximum Session Group Settings, page 10-53](#)
- [Maximum Session Global Settings, page 10-55](#)
- [Purging User Sessions, page 10-55](#)
- [Maximum User Session in Distributed Environment, page 10-56](#)

Maximum Login Failed Attempts Policy

ACS 5.8.1 allows the administrator to disable the user accounts after n successive failed attempts. You can configure the maximum login failed attempts count from ACS web interface. This feature is applicable only for internal users. You can configure this feature at user level, identity group level, and globally. ACS 5.8.1 introduces the maximum login failed attempt count configuration at user level and identity groups level. The global maximum login failed attempt count configuration is already available in ACS.



Note

ACS counts the failed attempts until you reach the maximum failed attempts count or make a successful login attempt. ACS does not have a specific time range (such as within 15 minutes, 30 minutes, 1 hour and so on) configured for consecutive failed attempts count calculation.



Note

If a user is configured with less number of maximum login failed attempt count and the user group is configured with more number of maximum login failed attempt count, then ACS considers the maximum login failed attempt count at the user level even though it is less.

When a user enters an incorrect login credentials, ACS executes the following maximum login failed attempts policy algorithm:

-
- Step 1** If the maximum login failed attempt count is configured at user level:
- ACS disables the user account if the maximum login failed attempts count is reached.
 - ACS allows the user to enter the credentials and try logging in again if the maximum login failed attempts count is not reached.
- If the maximum login failed attempt count is not configured at user level, then ACS proceeds to identity group level check.
- Step 2** If the maximum login failed attempt count is configured at the identity group that is associated with the user:
- ACS disables the user account if the maximum login failed attempts count is reached.

- ACS allows the user to enter the credentials and try logging in again if the maximum login failed attempts count is not reached.

If the maximum login failed attempt count is not configured at the immediate group that is associated with the user, then ACS proceeds to the parent identity group level.

Step 3 If the maximum login failed attempt count is configured at the parent identity group:

- ACS disables the user account if the maximum login failed attempts count is reached.
- ACS allows the user to enter the credentials and try logging in again if the maximum login failed attempts count is not reached.

If the maximum login failed attempt count is not configured at the parent group, then ACS proceeds to the next level in the hierarchy until it reaches the root of the hierarchical groups. If the maximum login failed attempt count is not configured at any group including the root, then ACS proceeds to the global maximum login failed attempt count check.

Step 4 If the maximum login failed attempts count is configured globally:

- ACS disables the user account if the maximum login failed attempts count is reached.
- ACS allows the user to enter the credentials and try logging in again if the maximum login failed attempts count is not reached.

If the global maximum login failed attempts count configuration is not available, then ACS never disables the user account and allows the user to enter the login credentials and try logging in again and again.

This section describes the following:

- [Configuring Maximum Login Failed Attempts Count for Users, page 10-58.](#)
- [Configuring Maximum Login Failed Attempts Count for Identity Groups, page 10-59.](#)
- [Configuring Maximum Login Failed Attempts Count for Users Globally, page 10-59](#)

Configuring Maximum Login Failed Attempts Count for Users

To configure maximum login failed attempt count for internal users:

Step 1 Choose **Users and Identity Stores > Internal Identity Store > Users**.

The Internal Users page appears.

Step 2 Perform one of the following actions:

- Click **Create**.
- Click the username to whom you want to configure the maximum login failed attempts count, or check the check box next to the name and click **Edit**.

Step 3 Check the **Disable account after *n* successive failed attempts** check box and enter the maximum login failed attempts count in the text box provided.

Step 4 Click **Submit**.

The maximum login failed attempt count for the selected user is configured. The Internal Users page appears with the new configuration.

Configuring Maximum Login Failed Attempts Count for Identity Groups

To configure failed attempts count for identity groups:

-
- Step 1** Choose **Access Policies > Max Login Failed Attempts Policy > Max Login Failed Attempts Group Settings**.
- All the configured identity groups are listed.
- Step 2** Check the check box next to the group name for which you want to configure the maximum login failed attempts count.
- Step 3** Click **Edit**.
- The Edit Identity Groups page appears with the identity group name and the description.
- Step 4** Check the **Disable account after n successive failed attempts** check box and enter the failed attempts count in the text box provided under **Max Login Failed Attempts Group Settings** area.
- Step 5** Click **Submit**.
- The maximum login failed attempt count for the selected identity group is configured.
-

Configuring Maximum Login Failed Attempts Count for Users Globally

To configure failed attempts count for users globally:

-
- Step 1** Choose **System Administration > Users > Authentication Settings > Advanced**.
- The User Authentication Settings page appears with the Advanced tab.
- Step 2** Check the **Disable account if** check box.
- Step 3** Check the **Failed Attempts Exceed** check box and enter the maximum login failed attempts count in the text box provided.
- Step 4** Click **Submit**.
- The maximum login failed attempt count for internal users is configured globally.
-



Note

If the authentication points of the primary and secondary instances are in different geographical locations, you can expect a delay in Distributed Deployment update across the Wide Area Network, thereby leading to a delayed update from the secondary instance to the primary instance. In this case, if you authenticate a user against a secondary instance in a deployment which is in a geographical location other than where the primary instance is located, the feature “Disable User after N failed attempt count” will not work properly.



Monitoring and Reporting in ACS

The Monitoring and Reports drawer appears in the primary web interface window and contains the Launch Monitoring and Report Viewer option.

The Monitoring and Report Viewer provides monitoring, reporting, and troubleshooting capabilities for the ACS servers in your network. You can extract consolidated log, configuration, and diagnostic data from one or more ACS servers for advanced reporting and troubleshooting purposes.

You can configure the network access devices (NADs) in your network to send syslog messages to the Monitoring and Report Viewer. To do this, you must configure the logging port on the NAD to UDP 20514.

For example, to enable a NAD in your network to send syslog messages to the Monitoring and Report Viewer, you must enter the following commands on the NAD through the CLI configuration mode:

- **logging monitor informational**
- **logging origin-id ip**
- **logging host *ip* transport udp port 20514**—where *ip* is the IP address of the Log Collector in your network.
- **epm logging**

Click **Launch Monitoring and Report Viewer** to open the Monitoring and Reports Viewer in a secondary web interface window, which contains these drawers:

- Monitoring and Reports
- Monitoring Configuration. (See [15, page 15-1](#).)

The Monitoring and Reports drawer provides the following functionality:

- **Dashboard**—Provides a high-level summary, updated in real time, of the ACS servers in the deployment, the authentication activity, and a summary of authentications against each identity store. See [Dashboard Pages, page 11-2](#).
- **Alarms**—You can define thresholds to represent acceptable system performance. Measurements are taken on an ongoing basis and compared against these thresholds. If the thresholds are exceeded, alarms are generated. See [Understanding Alarms, page 12-1](#).
- **Reports**—A rich set of reports are available. See [Managing Reports, page 13-1](#).
- **Troubleshooting**—Provides tools to assist in troubleshooting the ACS system, including tests for system connectivity and a tool to download support bundles. See [14, page 14-1](#).
- **Support for non-English characters (UTF-8)**—You can have non-English characters in:
 - Syslog messages—Configurable attribute value, user name, and ACS named configuration objects

- GUI input fields
- Query pages
- Reports
- Alarms
- Dashboard lookup
- Failure reason text

**Note**

In Monitoring and Reports drawer pages, you can use the page area's down arrow (v) to hide an area's content, and the right arrow (>) to show its content.

Related Topic

- [Authentication Records and Details, page 11-2](#)

Authentication Records and Details

A primary source of information for reports are the authentication records. Reports are provided that analyze these records according to multiple categories such as the Access Service used for the request, the user or host referenced in the request, the device making the request, etc. ACS provides summaries of the authentications per instance in each category, and administrators can get additional details.

Within each authentication record there is an option to view the details of the authentication record. The details contain the following information:

- Authentication Details—Full details of the authentication, which includes details from the request, the service, policies and rules selected for the requests, and the results returned in the response.
- Authentication Result—The contents of the result response.
- Steps—Lists the sequence of steps performed when processing the request.

The authentication details information is very helpful when trying to understand why a specific successful response was returned, or to track the steps performed when a failed response was returned.

Dashboard Pages

When you launch the Monitoring and Report Viewer, the Dashboard appears in a secondary web interface window.

ACS 5.8.1 provides a new customizable dashboard that contains tabs and portlets, where the Monitoring and Report Viewer consolidates your favorite queries, recent alarms and reports, and health status of ACS instances. Each of these tabs can have multiple portlets with each portlet containing an application of your choice.

You can select an application from the list the list of available applications. By default, the Monitoring and Report Viewer provides the following tabs and applications in the Dashboard:

**Note**


These tabs are customizable, and you can modify or delete the following tabs.

- General—The General tab lists the following:


- Five most recent alarms—When you click the name of the alarm, a dialog box appears with the details and the status of the alarm. You can update the information in the Status tab of this dialog box to track the alarm. See [Table 12-9](#) for a description of the fields in the Status tab.
- Favorite reports—The favorite reports are displayed in alphabetical order. To view a report, click the name of the report. You can view this report in the Interactive Viewer. You can customize this list to include your favorite reports and can quickly launch them from the dashboard.
- Troubleshooting—The Troubleshooting tab contains the following panes:
 - Live Authentications—View live authentications for the day. You can filter the records that appear in this pane.
 - My Links—You can add your favorite links to this pane.
 - NAD Show Command—You can run any show command on any NAD device from this pane. To run a NAD show command, you must:
 - a. Enter either the IPv4 or IPv6 IP address of the NAD (Required).
 - b. Enter the username and password for the NAD.
 - c. Choose the protocol, Telnet or SSHv2 (Required).
 - d. Enter the port number. The default is 23 (Required).
 - e. Enter the enable password.
 - f. Check the Use Console Server check box if you want to use the console server.
 - g. Enter either the Ipv4 or Ipv6 address of the console server—This field is required if you check the Use Console Server check box.
 - h. Enter the show command that you want to run on the NAD (Required).

When the Monitoring and Report Viewer executes the NAD show command, it might sometimes prompt you for additional details. See [Table 14-5](#) for a description of the fields in the Progress Details page. After you click **Done**, you can click **Show Results Summary** to view the result as shown in [Table 14-6](#).

- Authentication Lookup—You can use this portlet to run an authentication report with default parameters, find authentication records for a user or MAC address, and run user or endpoint summary report for a user or end point respectively. For more information on the Authentication Lookup Portlet, see [Working with the Authentication Lookup Portlet, page 11-5](#).
- Authentication Trends—The Authentication Trends tab contains the following panes:
 - Authentication Trend—Provides a graphical and tabular representation of the authentication trend for up to the past 30 days. In the graphical representation, the time is plotted on the X-axis and the authentications are plotted on the Y-axis.

The tabular representation provides the number of passed, failed, and dropped authentications for each day. The button at the lower-right corner of the chart () allows you to toggle between the two views.

- Top <N> Authentications—Provides a graphical representation of the top <N> authentications. Time is plotted on the X-axis and authentications are plotted on the Y-axis.
- Authentication Snapshot—Provides a snapshot of authentications in the graphical and tabular formats for up to the past 30 days. In the graphical representation, the field based on which the records are grouped together is plotted on the X-axis and the authentications are plotted on the Y-axis.

The tabular representation provides the Category; Pass Count; Daily, Weekly, or Monthly Pass Count; Fail Count; and Daily, Weekly, or Monthly Fail Count. The button at the lower-right corner of the chart () allows you to toggle between the two views.

- ACS Health—The ACS Health tab provides the system and AAA health of ACS instances. This information is available in a tabular format.
 - System status is determined by the following parameters—CPU utilization, memory utilization, disk input/output utilization, and disk usage for /opt and /local disk.
 - AAA status is determined by RADIUS and TACACS+ latency

Hovering the mouse over the legend (Critical, Warning, Healthy) provides the criteria that determines the status of the ACS instance. For a detailed graphical representation of the ACS instance health, click the name of the ACS instance. The ACS health summary report appears. You can view this report in the Interactive Viewer.

You can configure the tabs in the Dashboard to suit your needs. See [Configuring Tabs in the Dashboard, page 11-6](#) for more information on how to configure tabs in the Dashboard and add applications to the tabs.

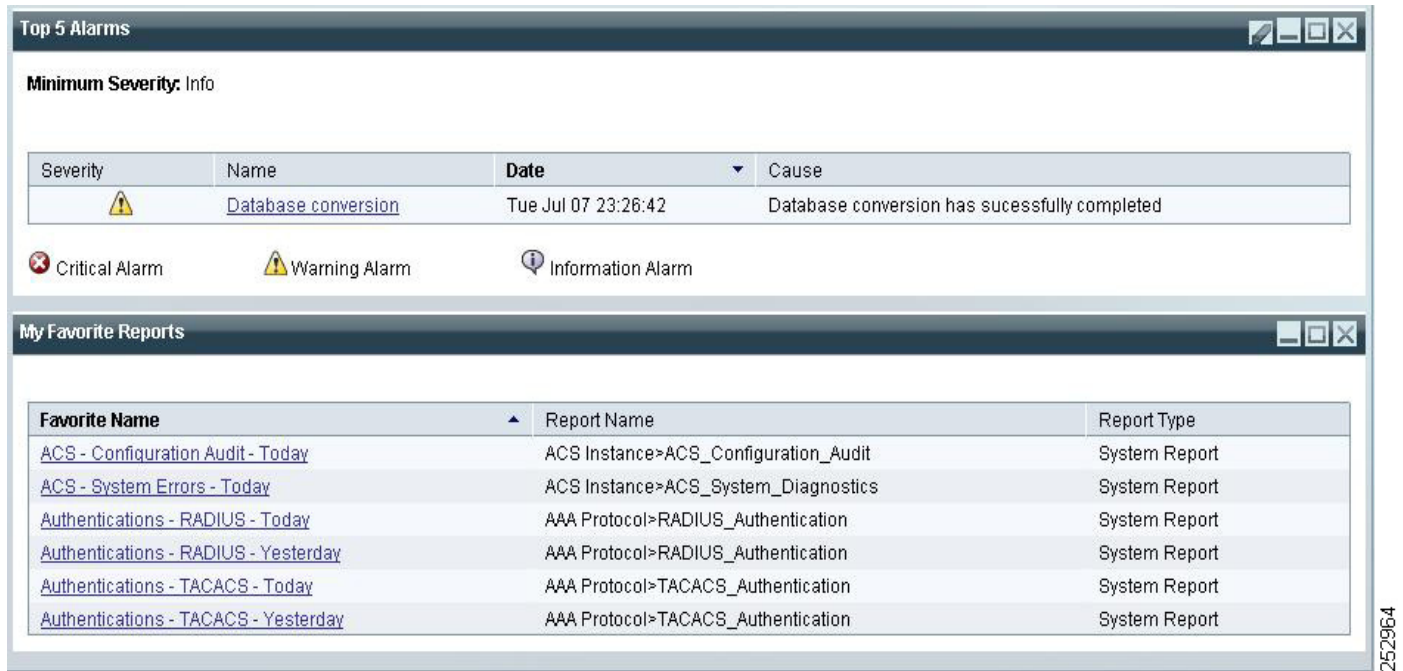
Related Topics

- [Working with Portlets, page 11-4](#)
- [Configuring Tabs in the Dashboard, page 11-6](#)
- [Adding Applications to Tabs, page 11-7](#)


Working with Portlets

A portlet is a small, self-contained window within a dashboard that displays information in the form of real-time charts, tabular reports, and so on. Each tab in the Dashboard consists of one or more portlets. [Figure 11-1](#) shows two portlets from the General tab.

Figure 11-1 Portlets



Top 5 Alarms and My Favorite Reports appear in separate windows. You can edit each of these portlets separately.

To edit a portlet, click the edit button () at the upper-right corner of the window. The Monitoring and Report Viewer allows you to customize the information in the portlets to suit your needs. You can add, edit, and delete tabs; edit application settings in portlets; and delete portlets.

Working with the Authentication Lookup Portlet

You can add the Authentication Lookup Portlet to the Dashboard.

To add the Authentication Lookup Portlet, see [Adding Applications to Tabs, page 11-7](#).

The Authentication Lookup Portlet contains the following fields:

- **Username/MAC Address**—(Required for summary reports) Username of the user or the MAC address in aa-bb-cc-dd-ee-ff format. The Monitoring and Report Viewer does not accept MAC address in any other format.
- **View**—Choose Authentication to run an authentication report or Summary for a summary report.
- **Time Range**—Depending on the View option that you choose, the Time Range drop-down list is populated. Choose the time range for which you want to generate the report.
- **Start Date**—(Enabled when you choose the Custom time range option) Choose the start date.
- **End Date**—(Enabled when you choose the Custom time range option) Choose the end date.
- **Protocol**—Choose either RADIUS or TACACS+ from the Protocol drop-down list. The protocol is not taken into account for endpoint summary reports.

Related Topics

- [Dashboard Pages, page 11-2](#)
- [Running the Authentication Lookup Report, page 11-6](#)

Running the Authentication Lookup Report

When you run an Authentication Lookup report, consider the following:

- If you have provided the username or MAC address value in the format aa-bb-cc-dd-ee-ff, an authentication report is run for this MAC address.
- If you have provided the username or MAC address value in any other format, the value is considered an username and authentication report is run for that user.
- If the Username or MAC address field is empty, an authentication report with default parameters is run for the chosen protocol and time range (similar to running a RADIUS or TACACS Authentication report in the catalog pages).
- If you provide a valid MAC address value for the Username or MAC address field and choose the Summary View option, an endpoint summary report is run. Irrespective of the protocol that you choose, an endpoint summary report is always run for the RADIUS protocol.

If the MAC address value that you provide is not in the prescribed format, it is assumed to be a username and a user authentication summary report is run for the chosen time range and protocol.

Configuring Tabs in the Dashboard

This section describes how to configure tabs in the Dashboard and add applications to it. This section contains:

- [Adding Tabs to the Dashboard, page 11-6](#)
- [Renaming Tabs in the Dashboard, page 11-7](#)
- [Changing the Dashboard Layout, page 11-8](#)
- [Deleting Tabs from the Dashboard, page 11-8](#)

Adding Tabs to the Dashboard

The Monitoring and Report Viewer Dashboard allows you to customize the tabs in the dashboard and the applications that are available from them. To add tabs to the Dashboard:

-
- Step 1** From the Monitoring and Report Viewer, choose **Monitoring and Reports > Dashboard**.
The Dashboard page appears.
 - Step 2** Click the **Configure** drop-down list at the upper-right corner of the Dashboard page.
 - Step 3** Click **Add New Page**.
 - Step 4** Enter the name of the tab that you want to create in the Add New Page text box.
 - Step 5** Click **Add Page**.

A new tab of your choice is created. You can add the applications that you most frequently monitor in this tab

Adding Applications to Tabs

To add an application to a tab:

-
- Step 1** From the Monitoring and Report Viewer > choose **Monitoring and Reports > Dashboard**.
The Dashboard page appears.
- Step 2** Select the tab to which you want to add an application.
If you want to add applications to a new tab, you must add the new tab to the Dashboard before you can add applications to it.
- Step 3** Click the **Configure** drop-down list at the upper-right corner of the Dashboard page.
- Step 4** Click **Add Application**.
An Add Application window appears.
- Step 5** Click **View Dashboard** to see the list of applications that you can add to the Dashboard.
Alternatively, you can enter the name of the application in the Search Content text box.
A list of applications appears.
- Step 6** Click the Add link the application that you want to add.
The application of your choice is added to the tab. You can edit the parameters in this tab.
-

Renaming Tabs in the Dashboard

To rename existing tabs in the Dashboard:

-
- Step 1** From the Monitoring and Report Viewer > choose **Monitoring and Reports > Dashboard**.
The Dashboard page appears.
- Step 2** Select the tab that you want to rename.
- Step 3** Click the **Configure** drop-down list at the upper-right corner of the Dashboard page.
- Step 4** Click **Rename Page**.
- Step 5** Enter the new name in the Rename Page text box.
- Step 6** Click **Update**.
The tab appears with the new name.
-


Changing the Dashboard Layout

You can change the look and feel of the Dashboard. ACS provides you with nine different in-built layouts. To choose a different layout:


-
- Step 1** From the Monitoring and Report Viewer, choose **Monitoring and Reports > Dashboard**.
The Dashboard page appears.
 - Step 2** Select the tab whose layout you wish to change.
 - Step 3** Click the **Configure** drop-down list at the upper-right corner of the Dashboard page.
A list of layout options appears.
 - Step 4** Click the radio button the layout style that you want for this tab.
 - Step 5** Click **Save** to change the layout.
-

Deleting Tabs from the Dashboard

To delete tabs from the Dashboard:

-
- Step 1** From the Monitoring and Report Viewer, choose **Monitoring and Reports > Dashboard**.
The Dashboard page appears.
 - Step 2** Click the **Configure** drop-down list at the upper-right corner of the Dashboard page.
 - Step 3** Click **Manage Pages**.
 - Step 4** Select the tab that you want to delete in the **Page Display Order** list box.
 - Step 5** Click  to delete the tab that you have selected.

**Note**

Alternatively, when you hover the mouse over the name of the tab that you want to delete, the following icon appears: . Click this icon to delete the tab.



Managing Alarms

The Monitoring feature in ACS generates alarms to notify you of critical system conditions. The monitoring component retrieves data from ACS. You can configure thresholds and rules on this data to manage alarms.

Alarm notifications are displayed in the web interface and you can get a notification of events through e-mail and Syslog messages. ACS filters duplicate alarms by default.

This chapter contains the following sections:

- [Understanding Alarms, page 12-1](#)
- [Viewing and Editing Alarms in Your Inbox, page 12-3](#)
- [Understanding Alarm Schedules, page 12-8](#)
- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Deleting Alarm Thresholds, page 12-36](#)
- [Configuring System Alarm Settings, page 12-37](#)
- [Understanding Alarm Syslog Targets, page 12-38](#)

Understanding Alarms

There are two types of alarms in ACS:

- [Threshold Alarms, page 12-1](#)
- [System Alarms, page 12-2](#)

Threshold Alarms

Threshold alarms are defined on log data collected from ACS servers that notify you of certain events. For example, you can configure threshold alarms to notify you of ACS system health, ACS process status, authentication activity or inactivity, and so on.

You define threshold conditions on these data sets. When a threshold condition is met, an alarm is triggered. While defining the threshold, you also define when the threshold should be applied (the time period), the severity of the alarm, and how the notifications should be sent.

Fifteen categories of available alarm thresholds allow you to monitor many different facets of ACS system behavior. See [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#) for more information on threshold alarms.

System Alarms

System alarms notify you of critical conditions encountered during the execution of the ACS Monitoring and Reporting viewer. System alarms also provide informational status of system activities, such as data purge events or failure of the log collector to populate the View database.

You cannot configure system alarms, which are predefined. However, you do have the option to disable system alarms or decide how you want to be notified if you have enabled them.

This section contains the following topics:

- [Evaluating Alarm Thresholds, page 12-2](#)
- [Notifying Users of Events, page 12-2](#)

Evaluating Alarm Thresholds

ACS evaluates the threshold conditions based on a schedule. You define these schedules and, while creating a threshold, you assign a schedule to it. A schedule consists of one or more continuous or noncontinuous periods of time during the week.

For example, you can create a schedule that is active from 8:00 a.m. to 5:00 p.m., Monday through Friday. See [Understanding Alarm Schedules, page 12-8](#) for more information. When you assign this schedule to a threshold, ACS evaluates the threshold and generates alarms only during the active period.

ACS evaluates the thresholds periodically depending on the number of thresholds that are currently enabled.

[Table 12-1](#) provides the length of the evaluation cycle for a given number of thresholds.

Table 12-1 *Evaluation Cycle of Alarm Thresholds*

Number of Enabled Thresholds	Evaluation Cycle ¹
1 to 20	Every 2 minutes
21 to 50	Every 3 minutes
51 to 100	Every 5 minutes

1. If the time taken to evaluate the thresholds increase, then the evaluation cycle increases from 2 to 3 minutes, 3 to 5 minutes, and from 5 to 15 minutes. The evaluation cycle time is reset to 2, 3, and 5 minutes every 12 hours.

When an evaluation cycle begins, ACS evaluates each enabled threshold one after another. If the schedule associated with the threshold allows the threshold to be executed, ACS evaluates the threshold conditions. An alarm is triggered if the condition is met. See [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#) for more information.

**Note**

System alarms do not have an associated schedule and are sent immediately after they occur. You can only enable or disable system alarms as a whole.

Notifying Users of Events

When a threshold is reached or a system alarm is generated, the alarm appears in the Alarms Inbox of the web interface. From this page, you can view the alarm details, add a comment about the alarm, and change its status to indicate that it is Acknowledged or Closed.

The alarm details in this page, wherever applicable, include one or more links to the relevant reports to help you investigate the event that triggered the alarm.

The Dashboard also displays the five most recent alarms. Alarms that you acknowledge or close are removed from this list in the Dashboard.

ACS provides you the option to receive notifications in the following formats:

- E-mail—Contains all the information that is present in the alarm details page. You can configure a list of recipients to whom this e-mail must be sent. ACS 5.8.1 provides you the option to receive notification of events through e-mail in HTML format.
- Syslog message—Sent to the Linux or Windows machines that you have configured as alarm syslog targets. You can configure up to two alarm syslog targets.

Viewing and Editing Alarms in Your Inbox

You can view alarms that ACS generates based on a threshold configuration or a rule on a set of data collected from ACS servers. Alarms that have met the configured thresholds are sent to your Inbox. After you view an alarm, you can edit the status of the alarm, assign the alarm to an administrator, and add notes to track the event.

To view an alarm in your Inbox, select **Monitoring and Reports > Alarms > Inbox**.

The Inbox page appears with a list of alarms that ACS triggered. [Table 12-2](#) describes the fields on the Alarms page. [Table 12-3](#) lists the system alarms in ACS 5.8.1 and its severity.

Table 12-2 *Alarms Page*

Option	Description
Severity	<p><i>Display only.</i> Indicates the severity of the associated alarm. Options are:</p> <ul style="list-style-type: none"> • Critical • Warning • Info
Name	Indicates the name of the alarm. Click to display the Alarms: Properties page and edit the alarm.
Time	<p><i>Display only.</i> Indicates the time of the associated alarm generation in the format <i>Ddd Mmm dd hh:mm:ss timezone yyyy</i>, where:</p> <ul style="list-style-type: none"> • Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. • Mmm = Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • dd = A two-digit numeric representation of the day of the month, from 01 to 31. • hh = A two-digit numeric representation of the hour of the day, from 00 to 23. • mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. • ss = A two-digit numeric representation of the second of the minute, from 00 to 59. • <i>timezone</i> = The time zone. • yyyy = A four-digit representation of the year.
Cause	<i>Display only.</i> Indicates the cause of the alarm.
Assigned To	<i>Display only.</i> Indicates who is assigned to investigate the alarm.

Table 12-2 Alarms Page (continued)

Option	Description
Status	<p><i>Display only.</i> Indicates the status of the alarm. Options are:</p> <ul style="list-style-type: none"> New—The alarm is new. Acknowledged—The alarm is known. Closed—The alarm is closed.
Edit	Check the check box the alarm that you want to edit, and click Edit to edit the status of the alarm and view the corresponding report.
Close	<p>Check the check box the alarm that you want to close, and click Close to close the alarm. You can enter closing notes before you close an alarm.</p> <p>Closing an alarm only removes the alarm from the dashboard. It does not delete the alarm.</p>
Delete	Check the check box the alarm that you want to delete, and click Delete to delete the alarm.

Table 12-3 System Alarms in ACS 5.8.1

Alarm	Severity
Purge Related Alarms	
Backup failed. Backup failed before Database Purge.	Critical
Backup successful. Backup failed before Database Purge.	Info
Database Purge for Daily Tables failed. Exception Details.	Critical
Database Purge for Monthly Tables failed. Exception Details.	Critical
Database Purge for Yearly Tables failed. Exception Details.	Critical
Incremental backup is not configured. Configuring incremental backup is necessary to make the database purge successful. This will help to avoid disk space issues. View database Size is file size in GB and size it occupies on the hard disk is actual db size in GB.	Warning
Configure Incremental Backup Data Repository as Remote Repository otherwise backup will fail and Incremental backup mode will be changed to off.	Warning
Configure Remote Repository under Purge Configuration which is used to take a backup of data before purge.	Warning
View database size exceeds the maximum limit of maxLimit GB. View database Size is file size GB and size it occupies on the hard disk is actualDBSize GB. View database size exceeds the max limit of maxLimit GB.	Critical
View database size exceeds the upper limit of upperLimit GB. View database Size is file size GB and size it occupies on the hard disk is actualDBSize GB. View database size exceeds the upper limit of upperLimit GB.	Critical
ACS View DB Size exceeds the lower limit lowerLimit GB. View database Size is file size GB and size it occupies on the hard disk is actualDBSize GB. View database size exceeds the lower limit of lowerLimit GB.	Warning
DB Purge. Database Start Purging.	Info
Disk Space Limit Exceeded - Window at : Disk Space Limit Exceeded recommended threshold at one month data. Now Purging week data till it reaches lower limit.	Warning

Table 12-3 System Alarms in ACS 5.8.1 (continued)

Alarm	Severity
ACS view Application Exceeded its Maximum Allowed Disk size. Disk Space Exceeded recommended threshold, extra monthsinnumber month(s) data purged.	Warning
ACS view Application Exceeded its Maximum Allowed Disk size. Disk Space Exceeded recommended threshold monthsinnumber month(s) data purged.	Info
Purge is successful. The size of records present in view data base is actualsizeinGB GB. The physical size of the view data base on the disk sizeinGB GB. If you want to reduce the physical size of the view data base, run acsview-db-compress command from acs-config mode through command line.	Warning
Purge process removed week week(s) data to reach lower limit	Info
Purge process was tried to remove maximum data to reach lower limit by purging last three weeks data but still acsview database size is having greater than lower limit. Currently we are keeping only last 1 week data.	Warning
The number of incoming log messages is reaching threshold value: GB's. Make sure that you configured ACS to send only the important category of messages to Log collector.	Warning
Incremental Backup	
On-demand Full Backup failed: Exception Details.	Critical
Full Database Backup failed. Exception Details.	Critical
Full Database Purge Backup failed. Exception Details.	Critical
Incremental Backup Failed. Exception Details.	Critical
Incremental Restore Successful.	Info
Incremental Restore failed. Reason: Exception Details	Critical
On-demand Full Backup failed: Exception Details	Critical
Full Database Backup failed: Exception Details.	Critical
Full Database Purge Backup failed: Exception Details	Critical
Incremental Backup Failed: Exception Details	Critical
Log Recovery	
Log Message Recovery failed: Exception Details	Critical
View Compress	
Database rebuild operation has started. The Log collector services would be shut down during this operation and they would be made up after rebuild operation is completed. If log recovery option is enabled already, any log messages that may be received during the rebuild operation would be recovered after log collector services are up.	Critical
The database reload operation completed.	Info
System detects a need to compress the database. Run the view database compress operation manually during maintenance window, otherwise, automatic database rebuild would be triggered to avoid disk space issue.	Warning
Automatic database rebuild operation has started. The Log collector services would be shut down during this operation and they would be made up after rebuild operation is completed. If log recovery option is enabled already, any log messages that may be received during the rebuild operation would be recovered after log collector services are up.	Critical
The database reload operation completed.	Info

Table 12-3 System Alarms in ACS 5.8.1 (continued)

Alarm	Severity
Automatic database rebuild operation would be triggered as the size of the database exceeds the limit to avoid disk space issue. Enable log recovery feature to recover missed log messages during database rebuild operation. Database re-build operation will not continue till log recovery feature enabled.	Warning
Threshold Executor	
Could not complete executing all thresholds in the allocated thresholdEvaluationInterval minute interval. Thresholds will be evaluated again in the next interval. This error could have happened because: The system is under heavy load (example: During Purging) There might be too many thresholds active at this time.	Info
Session Monitor	
Active sessions are over limit. Session is over 250000.	Warning
Syslog Collector Failure	
Please see Collector log for details.	Critical
Scheduled ACS Backup	
Scheduled backup of ACS configuration db failed to start due to invalid character in backup name.	Critical
Scheduled backup of ACS configuration db failed to start due to invalid repository. Please verify that repository exists.	Critical
Unable to get hostname. Scheduled backup of ACS configuration db failed. Please check ADE.log for more details.	Critical
Failed to load backup library. Scheduled backup of ACS configuration db failed. Please check ADE.log for more details.	Critical
Symbol lookup error. Scheduled backup of ACS configuration db failed. Please check ADE.log for more details.	Critical
Failed to perform ACS backup due to internal error. Please check ADE.log for more details.	Critical
System Diagnostics	
Secondary node stopped from processing replications.	Critical
Secondary node cannot establish communication channel against Primary node on Heartbeat/Replication/Replay topic.	Warning
Primary node cannot establish communication channel against secondary node on Heartbeat/Replication/Replay topic.	Warning
Heartbeat from Primary/Secondary indicates that Secondary is not synchronized with Primary for long time.	Warning
No heartbeat status is received from the secondary node for certain amount of time.	Warning
No heartbeat status is received from the primary node for certain amount of time.	Warning
Disk Size Check	
Backup of size directorySize M exceeds the allowed quota of MaxSize M. This will not prohibit backup process as long as there is enough disk space. Please note that this indicates you should consider moving ACS to a higher disk space machine.	Critical

Table 12-3 System Alarms in ACS 5.8.1 (continued)

Alarm	Severity
Patch of size directorySize M exceeds the allowed quota of MaxSize M. This will not prohibit patch installation process as long as there is enough disk space. Please note that this indicates you should consider moving ACS to a higher disk space machine.	Critical
Support bundle of size directorySize M exceeds the allowed quota of MaxSize M. This will not prohibit support bundle collection process as long as there is enough disk space. Please note that this indicates you should consider moving ACS to a higher disk space machine.	Critical
Backup of size directorySize M exceeds the allowed quota of MaxSize M. This will not prohibit restore process as long as there is enough disk space. Please note that this indicates you should consider moving ACS to a higher disk space machine.	Critical
Disk Quota	
ACS DB size has exceeded allowed quota.	Critical
ACS View DB size has exceeded allowed quota.	Critical
View Data Upgrade	
Database conversion has successfully completed. The View newVersion database has been upgraded to installedVersion and is ready for activation.	Warning
Database conversion did not complete successfully. The View newVersion upgrade process encountered errors and was not able to complete. The upgrade log contains detailed information.	Critical
Others	
Aggregator is busy. Dropping syslog.	Critical
Collector is busy. Dropping syslog.	Critical
Unregistered ACS Server servername.	Warning
Unknown Message code received.	Critical

**Note**

The Alarm for ACS database exceeding the quota is sent only when the total size of the ACS database exceeds the quota. Total size of ACS database = acs*.log + acs.db where acs*.log is the ACS database log file. Both the acs*.log and acs.db files are present under /opt/CSCOacs/db.

**Note**

ACS cannot be used as a remote syslog server. But, you can use an external server as a syslog server. If you use an external server as a syslog server, no alarms can be generated in the ACS view as the syslog messages are sent to the external syslog server. If you want to generate the alarms in ACS view, set the logging option as localhost using CLI.

To edit an alarm:

-
- Step 1** Select **Monitoring and Reports > Alarms > Inbox**.
- The Inbox page appears with a list of alarms that ACS triggered.
- Step 2** Check the check box the alarm that you want to edit and click **Edit**.
- The Inbox - Edit page appears with the following tabs:

- **Alarm**—This tab provides more information on the event that triggered the alarm. [Table 12-4](#) describes the fields in the Alarm tab. You cannot edit any of the fields in the Alarm tab.

Table 12-4 *Inbox - Alarm Tab*

Option	Description
Occurred At	Date and time when the alarm was triggered.
Cause	The event that triggered the alarm.
Detail	Additional details about the event that triggered the alarm. ACS usually lists the counts of items that exceeded the specified threshold.
Report Links	Wherever applicable, one or more hyperlinks are provided to the relevant reports that allow you to further investigate the event.
Threshold	Information on the threshold configuration.

- **Status**—This tab allows you to edit the status of the alarm and add a description to track the event.

Step 3 Modify the fields in the Status tab as required. [Table 12-5](#) describes the fields.

Table 12-5 *Inbox - Status Tab*

Option	Description
Status	Status of the alarm. When an alarm is generated, its status is New. After you view the alarm, change the status of the alarm to Acknowledged or Closed to indicate the current status of the alarm.
Assigned To	(Optional) Specify the name of the user to whom this alarm is assigned.
Notes	(Optional) Enter any additional information about the alarm that you want to record.

Step 4 Click **Submit** to save the changes.

The Alarms page appears with the changes you made.

Related Topics

- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Deleting Alarm Thresholds, page 12-36](#)

Understanding Alarm Schedules

You can create alarm schedules to specify when a particular alarm threshold is run. You can create, edit, and delete alarm schedules. You can create alarm schedules to be run at different times of the day during the course of a seven-day week.

By default, ACS comes with the non-stop alarm schedule. This schedule monitors events 24 hours a day, seven days a week.

To view a list of alarm schedules, choose **Monitoring and Reports > Alarms > Schedules**. The Alarm Schedules page appears. [Table 12-6](#) lists the fields in the Alarm Schedules page.

Table 12-6 Alarm Schedules Page

Option	Description
Filter	Enter a search criterion to filter the alarm schedules based on your search criterion.
Go	Click Go to begin the search.
Clear Filter	Click Clear Filter to clear the search results and list all the alarm schedules.
Name	The name of the alarm schedule.
Description	(Optional) A brief description of the alarm schedule.

This section contains the following topics:

- [Creating and Editing Alarm Schedules, page 12-9](#)
- [Assigning Alarm Schedules to Thresholds, page 12-10](#)
- [Deleting Alarm Schedules, page 12-10](#)

Creating and Editing Alarm Schedules

To create or edit an alarm schedule:

Step 1 Choose **Monitoring and Reports > Alarms > Schedules**.

The Alarm Schedules page appears.

Step 2 Do either of the following:

- Click **Create**.
- Check the check box the alarm schedule that you want to edit, then click **Edit**.

The Alarm Schedules - Create or Edit page appears. [Table 12-7](#) lists the fields in the Alarms Schedules - Create or Edit page.

Table 12-7 Alarm Schedules - Create or Edit Page

Option	Description
Identification	
Name	Name of the alarm schedule. The name can be up to 64 characters in length.
Description	A brief description of the alarm schedule; can be up to 255 characters in length.
Schedule	
Click a square to select or deselect that hour. Use the Shift key to select or deselect a block starting from the previous selection. For more information on schedule boxes, see Schedule Boxes, page 5-16 .	
Select All	Click Select All to create a schedule that monitors for events all through the week, 24 hours a day, 7 days a week.
Clear All	Click Clear All to deselect all the selection.
Undo All	When you edit a schedule, click Undo All to revert back to the previous schedule.

Step 3 Click **Submit** to save the alarm schedule.

The schedule that you create is added to the Schedule list box in the Threshold pages.

Assigning Alarm Schedules to Thresholds

When you create an alarm threshold, you must assign an alarm schedule for the threshold. To assign an alarm schedule:

Step 1 Choose **Monitoring and Reports > Alarms > Thresholds**.

The Thresholds page appears.



Note

This procedure only describes how to assign a schedule to a threshold. For detailed information on how to create, edit, or duplicate a threshold, see [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#).

Step 2 Do one of the following.

- Click **Create**.
- Check the check box the threshold that you want to edit and click **Edit**.
- Check the check box the threshold that you want to duplicate and click **Duplicate**.

Step 3 In the General tab, choose the schedule that you want from the Schedule drop-down list box.

Step 4 Click **Submit** to assign the schedule to the threshold.

Deleting Alarm Schedules



Note

Before you delete an alarm schedule, ensure that it is not referenced by any thresholds that are defined in ACS. You cannot delete the default schedule (nonstop) or schedules that are referenced by any thresholds.

To delete an alarm schedule:

Step 1 Choose **Monitoring and Reports > Alarms > Schedules**.

The Alarm Schedules page appears.

Step 2 Check the check box the alarm schedule that you want to delete, then click **Delete**.

The following message appears:

Are you sure you want to delete the selected item(s)?

Step 3 Click **Yes** to delete the alarm schedule.

The alarm schedule page appears without the schedule that you deleted.

Creating, Editing, and Duplicating Alarm Thresholds

Use this page to configure thresholds for each alarm category. You can configure up to 100 thresholds.

To configure a threshold for an alarm category:

Step 1 Select **Monitoring and Reports > Alarms > Thresholds**.

The Alarms Thresholds page appears as described in [Table 12-8](#):

Table 12-8 *Alarm Thresholds Page*

Option	Description
Name	The name of the alarm threshold.
Description	The description of the alarm threshold.
Category	The alarm threshold category. Options can be: <ul style="list-style-type: none">• Passed Authentications• Failed Authentications• Authentication Inactivity• TACACS Command Accounting• TACACS Command Authorization• ACS Configuration Changes• ACS System Diagnostics• ACS Process Status• ACS System Health• ACS AAA Health• RADIUS Sessions• Unknown NAD• External DB Unavailable• RBACL Drops• NAD-reported AAA Down
Last Modified Time	The time at which the alarm threshold was last modified by a user.
Last Alarm	The time at which the last alarm was generated by the associated alarm threshold.
Alarm Count	The number of times that an associated alarm was generated.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box the alarm that you want to duplicate, then click **Duplicate**.
- Click the alarm name that you want to modify, or check the check box the alarm that you want to modify, then click **Edit**.
- Check the check box the alarm that you want to enable, then click **Enable**.
- Check the check box the alarm that you want to disable, then click **Disable**.

- Step 3** Modify fields in the Thresholds page as required. See the following pages for information about valid field options:
- [Configuring General Threshold Information, page 12-16](#)
 - [Configuring Threshold Criteria, page 12-16](#)
 - [Configuring Threshold Notifications, page 12-35](#)
- Step 4** Click **Submit** to save your configuration.
- The alarm threshold configuration is saved. The Threshold page appears with the new configuration.
-

Related Topics

- [Configuring General Threshold Information, page 12-16](#)
- [Configuring Threshold Criteria, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

Alarm Threshold Messages

A general alarm threshold message would include the following:

```
<month> <date> <time> <acs instance name> <alarm category> <syslog id> <number of
fragments> <first fragment> <alarm threshold name = "Value">, <severity = "value">, <cause
= "value">, <Detail = "Other details">.
```

A sample alarm threshold message is given below:

```
<178> Apr 2 13:23:00 ACS Server1 0000000005 1 0 ACSVIEW_ALARM Threshold alarm name =
"System_Diagnostics", severity = Warn, cause = "Alarm caused by System_Diagnostics
threshold", detail = "(ACS Instance = ACS Server, Category =
CSCOacs_Internal_Operations_Diagnostics, Severity = Warn, Message Text = CTL for syslog
server certificate is empty)"
```

[Table 12-9](#) displays the list of all alarm threshold messages.

Table 12-9 List of Alarm Threshold Messages

Alarm Threshold Category	Alarm Header	Alarm Name	Severity	Cause	Details
Passed Authentication	<month> <date> <time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 00000001 Number of Fragments: 1 First Fragment: 0	Authentication	Critical/Warning/Info	This alarm is raised when the authentication threshold is reached.	User: user1 Passed authentication count: 2
Failed Authentication	<month> <date> <time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 00000002 Number of Fragments: 1 First Fragment: 0	Authentication	Critical/Warning/Info	This alarm is raised when the authentication threshold is reached.	User: user1 Failed authentication count: 2
Authentication Inactivity	<month> <date> <time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 000000081 Number of Fragments: 1 First Fragment: 0	Authentication inactivity	Critical/Warning/Info	This alarm is raised when the authentication inactivity has occurred.	Following ACS instance(s) did not receive any authentication request between <month> <date> <time> <timezone> <year> and <month> <date> <time> <timezone> <year>: acsserver1
TACACS Command Accounting	<month> <date> <time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 0000000127 Number of Fragments: 1 First Fragment: 0	TACACS Accounting	Critical/Warning/Info	This alarm is caused when the TACACS+ accounting threshold is reached.	ACS instance: acsserver1 Time: <month> <date> <time> <timezone> <year> User: user1 Privilege: 0 Command: CmdAV = show run

Table 12-9 List of Alarm Threshold Messages (continued)

Alarm Threshold Category	Alarm Header	Alarm Name	Severity	Cause	Details
TACACS Command Authorization	<p><month> <date> <time> <acs instance name></p> <p>Alarm Category: CSCOacs_View_Alarm</p> <p>Syslog ID: 0000000128</p> <p>Number of Fragments: 1</p> <p>First Fragment: 0</p>	TACACS Authorization	Critical/Warning/Info	This alarm is caused when the TACACS+ authorization threshold is reached.	<p>ACS instance: acsserver1</p> <p>Time: <month> <date> <time> <timezone> <year></p> <p>Network Device: device1</p> <p>User: user1</p> <p>Privilege: 0</p> <p>Command: CmdAV = show run</p> <p>Authorization Result: Passed</p> <p>Identity Group: All Groups,</p> <p>Device Group & Device Type: All Device Types</p> <p>Location: All Locations</p>
ACS Configuration Changes	<p><month> <date> <time> <acs instance name></p> <p>Alarm Category: CSCOacs_View_Alarm</p> <p>Syslog ID: 0000000002</p> <p>Number of Fragments: 1</p> <p>First Fragment: 0</p>	Configuration Changes	Critical/Warning/Info	This alarm is caused when the configuration changes threshold is reached.	<p>ACS instance: acsserver1</p> <p>Time: <month> <date> <time> <timezone> <year></p> <p>Administrator: acsadmin</p> <p>Object Name: ACSAdmin</p> <p>Object Type: Administrator Account</p> <p>Change: UPDATE</p>
ACS System Diagnostics	<p><month> <date> <time> <acs instance name></p> <p>Syslog ID: 0000000005</p> <p>Number of Fragments: 1</p> <p>First Fragment: 0</p>	System Diagnostics	Critical/Warning/Info	This alarm is caused when the system diagnostics threshold is reached.	<p>ACS instance: acsserver1</p> <p>Category: CSCOacs_Internal_Operations_Diagnostics</p> <p>Severity: warning</p> <p>Message Text: CTL for Syslog server certificate is empty</p>

Table 12-9 List of Alarm Threshold Messages (continued)

Alarm Threshold Category	Alarm Header	Alarm Name	Severity	Cause	Details
ACS Process Status	<month> <date> <time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 0000000001 Number of Fragments: 1 First Fragment: 0	Authentication	Critical/Warning/Info	This alarm is caused when the authentication threshold is reached.	No process status updates have been received since the ACS View may be down.
ACS System Health	<month> <date> <time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 0000000004 Number of Fragments: 1 First Fragment: 0	Authentication	Critical/Warning/Info	This alarm is caused when the authentication threshold is reached.	ACS instance: acsserver1 CPU utilization(%): 0.96 Memory utilization(%): 91.73 Disk space used /opt(%): 14.04 Disk space used /localdisk(%): 8.94
ACS AAA Health	<month> <date> <time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 0000000003 Number of Fragments: 1 First Fragment: 0	AAA Health	Critical/Warning/Info	This alarm is caused when the AAA health threshold is reached.	ACS instance: acsserver1 RADIUS throughput (transactions per second): 0.00
RADIUS Sessions	<month> <date> <time> <acs instance name> Syslog ID: 0000000003 Number of Fragments: 1 First Fragment: 0	RADIUS Session	Critical/Warning/Info	This alarm is caused when the RADIUS sessions threshold is reached.	ACS instance: acsserver1 Device IP: 192.168.1.2 Count: 12
Unknown NAD	<month> <date> <time> <acs instance name> Syslog ID: 0000000002 Number of Fragments: 1 First Fragment: 0	Unknown NAD	Critical/Warning/Info	This alarm is caused when the unknown NAD threshold is reached.	ACS instance: acsserver1 Unknown NAD count: 12

Table 12-9 List of Alarm Threshold Messages (continued)

Alarm Threshold Category	Alarm Header	Alarm Name	Severity	Cause	Details
External Database Unavailable	<month> <date> <time> <acs instance name> Alarm Category: CSCOacs_View_Alarm Syslog ID: 0000000001 Number of Fragments: 1 First Fragment: 0	External database	Critical/Warning/Info	This alarm is caused when the external database threshold is reached.	ACS instance: acsserver1 External database unavailable: 6
NAD-reported AAA Down	<month> <date> <time> <acs instance name> Syslog ID: 0000000004 Number of Fragments: 1 First Fragment: 0	NAD_Reported_AAA_Down	Critical/Warning/Info	This alarm is caused when the NAD_Reported_AAA_Down threshold is reached.	ACS instance: acsserver1 AAA down count: 10

Configuring General Threshold Information

To configure general threshold information, fill out the fields in the General Tab of the Thresholds page. [Table 12-10](#) describes the fields.

Table 12-10 General Tab

Option	Description
Name	Name of the threshold.
Description	(Optional) The description of the threshold.
Enabled	Check this check box to allow this threshold to be executed.
Schedule	Use the drop-down list box to select a schedule during which the threshold should be run. A list of available schedules appears in the list.

Related Topics

- [Configuring Threshold Criteria, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

Configuring Threshold Criteria

ACS 5.8.1 provides the following threshold categories to define different threshold criteria:

- [Passed Authentications, page 12-17](#)
- [Failed Authentications, page 12-19](#)
- [Authentication Inactivity, page 12-21](#)
- [TACACS Command Accounting, page 12-22](#)

- [TACACS Command Authorization, page 12-23](#)
- [ACS Configuration Changes, page 12-24](#)
- [ACS System Diagnostics, page 12-25](#)
- [ACS Process Status, page 12-26](#)
- [ACS System Health, page 12-27](#)
- [ACS AAA Health, page 12-28](#)
- [RADIUS Sessions, page 12-29](#)
- [Unknown NAD, page 12-30](#)
- [External DB Unavailable, page 12-31](#)
- [RBACL Drops, page 12-32](#)
- [NAD-Reported AAA Downtime, page 12-34](#)

Passed Authentications

When ACS evaluates this threshold, it examines the RADIUS or TACACS+ passed authentications that occurred during the time interval that you have specified up to the previous 24 hours.

These authentication records are grouped by a common attribute, such as ACS Instance, User, Identity Group, and so on. The number of records within each of these groups is computed. If the count computed for any of these groups exceeds the specified threshold, an alarm is triggered.

For example, if you configure a threshold with the following criteria: Passed authentications greater than 1000 in the past 20 minutes for an ACS instance. When ACS evaluates this threshold and three ACS instances have processed passed authentications as follows:

ACS Instance	Passed Authentication Count
New York ACS	1543
Chicago ACS	879
Los Angeles	2096

An alarm is triggered because at least one ACS instance has greater than 1000 passed authentications in the past 20 minutes.



Note

You can specify one or more filters to limit the passed authentications that are considered for threshold evaluation. Each filter is associated with a particular attribute in the authentication records and only those records whose filter value matches the value that you specify are counted. If you specify multiple filters, only the records that match all the filter conditions are counted.

Modify the fields in the Criteria tab as described in [Table 12-11](#) to create a threshold with the passed authentication criteria.

Table 12-11 Passed Authentications

Option	Description
Passed Authentications	<p>Enter data according to the following: greater than <i>count</i> > occurrences % > in the past <i>time</i> > Minutes Hours for a <i>object</i>, where:</p> <ul style="list-style-type: none"> <i>count</i> values can be the absolute number of occurrences or percent. Valid values are: <ul style="list-style-type: none"> <i>count</i> must be in the range 0 to 99 for greater than. <i>count</i> must be in the range 1 to 100 for lesser than. occurrences % > value can be occurrences or %. <i>time</i> values can be 1 to 1440 minutes, or 1 to 24 hours. Minutes Hours value can be Minutes or Hours. <i>object</i> values can be: <ul style="list-style-type: none"> ACS Instance User Identity Group Device IP Identity Store Access Service NAD Port AuthZ Profile AuthN Method EAP AuthN EAP Tunnel <p>In a distributed deployment, if there are two ACS instances, the count is calculated as an absolute number or as a percentage for each of the instances. ACS triggers an alarm only when the individual count of any of the ACS instance exceeds the specified threshold.</p>
Filter	
ACS Instance	Click Select to choose a valid ACS instance on which to configure your threshold.
User	Click Select to choose or enter a valid username on which to configure your threshold.
Identity Group	Click Select to choose a valid identity group name on which to configure your threshold.
Device Name	Click Select to choose a valid device name on which to configure your threshold.
Device IP	Click Select to choose or enter a valid device IP address on which to configure your threshold.
Device Group	Click Select to choose a valid device group name on which to configure your threshold.
Identity Store	Click Select to choose a valid identity store name on which to configure your threshold.
Access Service	Click Select to choose a valid access service name on which to configure your threshold.
MAC Address	Click Select to choose or enter a valid MAC address on which to configure your threshold. This filter is available only for RADIUS authentications.
NAD Port	Click Select to choose a port for the network device on which to configure your threshold. This filter is available only for RADIUS authentications.

Table 12-11 *Passed Authentications (continued)*

Option	Description
AuthZ Profile	Click Select to choose an authorization profile on which to configure your threshold. This filter is available only for RADIUS authentications.
AuthN Method	Click Select to choose an authentication method on which to configure your threshold. This filter is available only for RADIUS authentications.
EAP AuthN	Click Select to choose an EAP authentication value on which to configure your threshold. This filter is available only for RADIUS authentications.
EAP Tunnel	Click Select to choose an EAP tunnel value on which to configure your threshold. This filter is available only for RADIUS authentications.
Protocol	Use the drop-down list box to configure the protocol that you want to use for your threshold. Valid options are: <ul style="list-style-type: none"> • RADIUS • TACACS+

Related Topics

- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Configuring General Threshold Information, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

Failed Authentications

When ACS evaluates this threshold, it examines the RADIUS or TACACS+ failed authentications that occurred during the time interval that you have specified up to the previous 24 hours. These authentication records are grouped by a common attribute, such as ACS Instance, User, Identity Group, and so on.

The number of records within each of these groups is computed. If the count computed for any of these groups exceeds the specified threshold, an alarm is triggered.

For example, if you configure a threshold with the following criteria: Failed authentications greater than 10 in the past 2 hours for Device IP. When ACS evaluates this threshold, if failed authentications have occurred for four IP addresses in the past two hours as follows:

Device IP	Failed Authentication Count
a.b.c.d	13
e.f.g.h	8
i.j.k.l	1
m.n.o.p	1

An alarm is triggered because at least one Device IP has greater than 10 failed authentications in the past 2 hours.

**Note**

You can specify one or more filters to limit the failed authentications that are considered for threshold evaluation. Each filter is associated with a particular attribute in the authentication records and only those records whose filter value matches the value that you specify are counted. If you specify multiple filters, only the records that match all the filter conditions are counted.

Modify the fields in the Criteria tab as described in [Table 12-12](#) to create a threshold with the failed authentication criteria.

Table 12-12 *Failed Authentications*

Option	Description
Failed Authentications	<p>Enter data according to the following:</p> <p>greater than <i>count</i> > occurrences % > in the past <i>time</i> > <i>Minutes</i> <i>Hours</i> for a <i>object</i>, where:</p> <ul style="list-style-type: none"> <i>count</i> values can be the absolute number of occurrences or percent. Valid values must be in the range 0 to 99. occurrences % > value can be occurrences or %. <i>time</i> values can be 1 to 1440 minutes, or 1 to 24 hours. <i>Minutes</i> <i>Hours</i> value can be Minutes or Hours. <i>object</i> values can be: <ul style="list-style-type: none"> ACS Instance User Identity Group Device IP Identity Store Access Service NAD Port AuthZ Profile AuthN Method EAP AuthN EAP Tunnel <p>In a distributed deployment, if there are two ACS instances, the count is calculated as an absolute number or as a percentage for each of the instances. ACS triggers an alarm only when the individual count of any of the ACS instance exceeds the specified threshold.</p>
Filter	
Failure Reason	Click Select to enter a valid failure reason name on which to configure your threshold.
ACS Instance	Click Select to choose a valid ACS instance on which to configure your threshold.
User	Click Select to choose or enter a valid username on which to configure your threshold.
Identity Group	Click Select to choose a valid identity group name on which to configure your threshold.
Device Name	Click Select to choose a valid device name on which to configure your threshold.
Device IP	Click Select to choose or enter a valid device IP address on which to configure your threshold.

Table 12-12 Failed Authentications (continued)

Option	Description
Device Group	Click Select to choose a valid device group name on which to configure your threshold.
Identity Store	Click Select to choose a valid identity store name on which to configure your threshold.
Access Service	Click Select to choose a valid access service name on which to configure your threshold.
MAC Address	Click Select to choose or enter a valid MAC address on which to configure your threshold. This filter is available only for RADIUS authentications.
NAD Port	Click Select to choose a port for the network device on which to configure your threshold. This filter is available only for RADIUS authentications.
AuthZ Profile	Click Select to choose an authorization profile on which to configure your threshold. This filter is available only for RADIUS authentications.
AuthN Method	Click Select to choose an authentication method on which to configure your threshold. This filter is available only for RADIUS authentications.
EAP AuthN	Click Select to choose an EAP authentication value on which to configure your threshold. This filter is available only for RADIUS authentications.
EAP Tunnel	Click Select to choose an EAP tunnel value on which to configure your threshold. This filter is available only for RADIUS authentications.
Protocol	Use the drop-down list box to configure the protocol that you want to use for your threshold. Valid options are: <ul style="list-style-type: none"> • RADIUS • TACACS+

Related Topics

- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Configuring General Threshold Information, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

Authentication Inactivity

When ACS evaluates this threshold, it examines the RADIUS or TACACS+ authentications that occurred during the time interval that you have specified up to the previous 31 days. If no authentications have occurred during the specified time interval, an alarm is triggered.

You can specify filters to generate an alarm if no authentications are seen for a particular ACS instance or device IP address during the specified time interval.

If the time interval that you have specified in the authentication inactivity threshold is lesser than that of the time taken to complete an aggregation job, which is concurrently running, then this alarm is suppressed.

The aggregation job begins at 00:05 hours every day. From 23:50 hours, up until the time the aggregation job completes, the authentication inactivity alarms are suppressed.

For example, if your aggregation job completes at 01:00 hours today, then the authentication inactivity alarms will be suppressed from 23:50 hours until 01:00 hours.

**Note**

If you install ACS between 00:05 hours and 05:00 hours, or if you have shut down your appliance for maintenance at 00:05 hours, then the authentication inactivity alarms are suppressed until 05:00 hours.

Choose this category to define threshold criteria based on authentications that are inactive. Modify the fields in the **Criteria** tab as described in [Table 12-13](#).

Table 12-13 *Authentication Inactivity*

Option	Description
ACS Instance	Click Select to choose a valid ACS instance on which to configure your threshold.
Device	Click Select to choose a valid device on which to configure your threshold.
Protocol	Use the drop-down list box to configure the protocol that you want to use for your threshold. Valid options are: <ul style="list-style-type: none"> RADIUS TACACS+
Inactive for	Use the drop-down list box to select one of these valid options: <ul style="list-style-type: none"> Hours—Specify the number of hours in the range from 1 to 744. Days—Specify the number of days from 1 to 31.

Related Topics

- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Configuring General Threshold Information, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

TACACS Command Accounting

When ACS evaluates this threshold, it examines the TACACS+ accounting records that it received during the interval between the previous and current alarm evaluation cycle.

If one or more TACACS+ accounting records match, it calculates the time that has elapsed since the previous alarm evaluation cycle. When it reaches two, three, or five minutes depending on the number of active thresholds, ACS examines the TACACS+ accounting records received during the interval between the previous and current alarm evaluation cycle. I

If one or more TACACS+ accounting records match a specified command and privilege level, an alarm is triggered.

You can specify one or more filters to limit the accounting records that are considered for threshold evaluation. Each filter is associated with a particular attribute in the records, and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on TACACS commands. Modify the fields in the **Criteria** tab as described in [Table 12-14](#).

Table 12-14 TACACS Command Accounting

Option	Description
Command	Enter a TACACS command on which you want to configure your threshold.
Privilege	Use the drop-down list box to select the privilege level on which you want to configure your threshold. Valid options are: <ul style="list-style-type: none"> Any A number from 0 to 15.
Filter	
User	Click Select to choose or enter a valid username on which to configure your threshold.
Device Name	Click Select to choose a valid device name on which to configure your threshold.
Device IP	Click Select to choose or enter a valid device IP address on which to configure your threshold.
Device Group	Click Select to choose a valid device group name on which to configure your threshold.

Related Topics

- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Configuring General Threshold Information, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

TACACS Command Authorization

When ACS evaluates this threshold, it examines the TACACS+ accounting records that it received during the interval between the previous and current alarm evaluation cycle.

If one or more TACACS+ accounting records match, it calculates the time that has lapsed since the previous alarm evaluation cycle. When it reaches two, three, or five minutes depending on the number of active thresholds, ACS examines the TACACS+ authorization records received during the interval between the previous and current alarm evaluation cycle.

If one or more TACACS+ authorization records match a specified command, privilege level, and passed or failed result, an alarm is triggered.

You can specify one or more filters to limit the authorization records that are considered for threshold evaluation. Each filter is associated with a particular attribute in the records, and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on TACACS command authorization profile. Modify the fields in the **Criteria** tab as described in [Table 12-15](#).

Table 12-15 TACACS Command Authorization

Option	Description
Command	Enter a TACACS command on which you want to configure your threshold.
Privilege	Use the drop-down list box to select the privilege level on which you want to configure your threshold. Valid options are: <ul style="list-style-type: none"> Any A number from 0 to 15.

Table 12-15 TACACS Command Authorization (continued)

Option	Description
Authorization Result	Use the drop-down list box to select the authorization result on which you want to configure your threshold. Valid options are: <ul style="list-style-type: none"> Passed Failed
Filter	
User	Click Select to choose or enter a valid username on which to configure your threshold.
Identity Group	Click Select to choose a valid identity group name on which to configure your threshold.
Device Name	Click Select to choose a valid device name on which to configure your threshold.
Device IP	Click Select to choose or enter a valid device IP address on which to configure your threshold.
Device Group	Click Select to choose a valid device group name on which to configure your threshold.

Related Topics

- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Configuring General Threshold Information, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

ACS Configuration Changes

When ACS evaluates this threshold, it examines the accounting records that it received during the interval between the previous and current alarm evaluation cycle.

If one or more accounting records match, it calculates the time that has lapsed since the previous alarm evaluation cycle. When it reaches two, three, or five minutes depending on the number of active thresholds, ACS examines the ACS configuration changes made during the interval between the previous and current alarm evaluation cycle. If one or more changes were made, an alarm is triggered.

You can specify one or more filters to limit which configuration changes are considered for threshold evaluation. Each filter is associated with a particular attribute in the records, and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on configuration changes made in the ACS instance. Modify the fields in the **Criteria** tab as described in [Table 12-16](#).

Table 12-16 ACS Configuration Changes

Option	Description
Administrator	Click Select to choose a valid administrator username on which you want to configure your threshold.
Object Name	Enter the name of the object on which you want to configure your threshold.
Object Type	Click Select to choose a valid object type on which you want to configure your threshold.

Table 12-16 ACS Configuration Changes

Option	Description
Change	Use the drop-down list box to select the administrative change on which you want to configure your threshold. Valid options are: <ul style="list-style-type: none">• Any• Create—Includes “duplicate” and “edit” administrative actions.• Update• Delete
Filter	
ACS Instance	Click Select to choose a valid ACS instance on which to configure your threshold.

Related Topics

- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Configuring General Threshold Information, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

ACS System Diagnostics

When ACS evaluates this threshold, it examines the accounting records that it received during the interval between the previous and current alarm evaluation cycle.

If one or more accounting records match, it calculates the time that has lapsed since the previous alarm evaluation cycle. When it reaches two, three, or five minutes depending on the number of active thresholds, ACS examines system diagnostic records generated by the monitored ACS during the interval.

If one or more diagnostics were generated at or above the specified security level, an alarm is triggered. You can specify one or more filters to limit which system diagnostic records are considered for threshold evaluation.

Each filter is associated with a particular attribute in the records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on system diagnostics in the ACS instance. Modify the fields in the **Criteria** tab as described in [Table 12-17](#).

Table 12-17 ACS System Diagnostics

Option	Description
Severity at and above	Use the drop-down list box to choose the severity level on which you want to configure your threshold. This setting captures the indicated severity level and those that are higher within the threshold. Valid options are: <ul style="list-style-type: none"> Fatal Error Warning Info Debug
Message Text	Enter the message text on which you want to configure your threshold. Maximum character limit is 1024.
Filter	
ACS Instance	Click Select to choose a valid ACS instance on which to configure your threshold.

Related Topics

- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Configuring General Threshold Information, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

ACS Process Status

When ACS evaluates this threshold, it examines the accounting records that it received during the interval between the previous and current alarm evaluation cycle.

If one or more accounting records match, it calculates the time that has lapsed since the previous alarm evaluation cycle. When it reaches two, three, or five minutes depending on the number of active thresholds, ACS determines whether any ACS process has failed during that time.

If ACS detects one or more failures, an alarm is triggered. You can limit the check to particular processes or a particular ACS instance or both.

Choose this category to define threshold criteria based on ACS process status. Modify the fields in the **Criteria** tab as described in [Table 12-18](#).

Table 12-18 ACS Process Status

Option	Description
Monitor Processes	
ACS Database	Check the check box to add the ACS database to your threshold configuration.
ACS Management	Check the check box to add the ACS management to your threshold configuration.
ACS Runtime	Check the check box to add the ACS runtime to your threshold configuration.
Monitoring and Reporting Database	Check the check box to have this process monitored. If this process goes down, an alarm is generated.

Table 12-18 ACS Process Status (continued)

Option	Description
Monitoring and Reporting Collector	Check the check box to have this process monitored. If this process goes down, an alarm is generated.
Monitoring and Reporting Alarm Manager	Check the check box to have this process monitored. If this process goes down, an alarm is generated.
Monitoring and Reporting Job Manager	Check the check box to have this process monitored. If this process goes down, an alarm is generated.
Monitoring and Reporting Log Processor	Check the check box to have this process monitored. If this process goes down, an alarm is generated.
Filter	
ACS Instance	Click Select to choose a valid ACS instance on which to configure your threshold.

Related Topics

- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Configuring General Threshold Information, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

ACS System Health

When ACS evaluates this threshold, it examines whether any system health parameters have exceeded the specified threshold in the specified time interval up to the previous 60 minutes. These health parameters include percentage of CPU utilization, percentage of memory consumption, and so on.

If any of the parameters exceed the specified threshold, an alarm is triggered. By default, the threshold applies to all ACS instances in your deployment. If you want, you can limit the check to just a single ACS instance.

Choose this category to define threshold criteria based on the system health of ACS. Modify the fields in the **Criteria** tab as described in [Table 12-19](#).

Table 12-19 ACS System Health

Option	Description
Average over the past	Use the drop-down list box to select the amount of time you want to configure for your configuration, where <min> is minutes and can be: <ul style="list-style-type: none"> • 15 • 30 • 45 • 60
CPU	Enter the percentage of CPU usage you want to set for your threshold configuration. The valid range is from 1 to 100.
Memory	Enter the percentage of memory usage (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.

Table 12-19 ACS System Health (continued)

Option	Description
Disk I/O	Enter the percentage of disk usage you want to set (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Disk Space Used/opt	Enter the percentage of /opt disk space usage you want to set (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Disk Space Used/local disk	Enter the percentage of local disk space usage you want to set (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Disk Space Used/	Enter the percentage of the / disk space usage you want to set (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Disk Space Used/tmp	Enter the percentage of temporary disk space usage you want to set (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 100.
Filter	
ACS Instance	Click Select to choose a valid ACS instance on which to configure your threshold.

Related Topics

- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Configuring General Threshold Information, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

ACS AAA Health

When ACS evaluates this threshold, it examines whether any ACS health parameters have exceeded the specified threshold in the specified time interval up to the previous 60 minutes. ACS monitors the following parameters:

- RADIUS Throughput
- TACACS Throughput
- RADIUS Latency
- TACACS Latency

If any of the parameters exceed the specified threshold, an alarm is triggered. By default, the threshold applies to all monitored ACS instances in your deployment. If you want, you can limit the check to just a single ACS instance.

Modify the fields in the **Criteria** tab as described in [Table 12-20](#).

Table 12-20 ACS AAA Health

Option	Description
Average over the past	Use the drop-down list box to select the amount of time you want to configure for your configuration, where <min> is minutes and can be: <ul style="list-style-type: none"> • 15 • 30 • 45 • 60
RADIUS Throughput	Enter the number of RADIUS transactions per second you want to set (lesser than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 999999.
TACACS Throughput	Enter the number of TACACS+ transactions per second you want to set (lesser than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 999999.
RADIUS Latency	Enter the number in milliseconds you want to set for RADIUS latency (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 999999.
TACACS Latency	Enter the number in milliseconds you want to set for TACACS+ latency (greater than or equal to the specified value) for your threshold configuration. The valid range is from 1 to 999999.
Filter	
ACS Instance	Click Select to choose a valid ACS instance on which to configure your threshold.

Related Topics

- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Configuring General Threshold Information, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

RADIUS Sessions

When ACS evaluates this threshold, it determines whether any authenticated RADIUS sessions have occurred in the past 15 minutes where an accounting start event has not been received for the session. These events are grouped by device IP address, and if the count of occurrences for any device IP exceeds the specified threshold, an alarm is triggered. You can set a filter to limit the evaluation to a single device IP.

Choose this category to define threshold criteria based on RADIUS sessions. Modify the fields in the **Criteria** tab as described in [Table 12-21](#).

Table 12-21 RADIUS Sessions

Option	Description
More than <i>num</i> authenticated sessions in the past 15 minutes, where accounting start event has not been received for a Device IP	<i>num</i> —A count of authenticated sessions in the past 15 minutes.
Filter	
ACS Instance	Click Select to choose a valid ACS instance on which to configure your threshold.
Device IP	Click Select to choose or enter a valid device IP address on which to configure your threshold.

Unknown NAD

When ACS evaluates this threshold, it examines the RADIUS or TACACS+ failed authentications that have occurred during the specified time interval up to the previous 24 hours. From these failed authentications, ACS identifies those with the failure reason Unknown NAD.

The unknown network access device (NAD) authentication records are grouped by a common attribute, such as ACS instance, user, and so on, and a count of the records within each of those groups is computed. If the count of records for any group exceeds the specified threshold, an alarm is triggered. This can happen if, for example, you configure a threshold as follows:

Unknown NAD count greater than 5 in the past 1 hour for a Device IP

If in the past hour, failed authentications with an unknown NAD failure reason have occurred for two different device IP addresses as shown in the following table, an alarm is triggered, because at least one device IP address has a count greater than 5.

Device IP	Count of Unknown NAD Authentication Records
a.b.c.d	6
e.f.g.h	1

You can specify one or more filters to limit the failed authentications that are considered for threshold evaluation. Each filter is associated with a particular attribute in the records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on authentications that have failed because of an unknown NAD. Modify the fields in the **Criteria** tab as described in [Table 12-22](#).

Table 12-22 Unknown NAD

Option	Description
Unknown NAD count	greater than <i>num</i> in the past <i>time Minutes Hours</i> for a <i>object</i> , where: <ul style="list-style-type: none"> <i>num</i> values can be any five-digit number greater than or equal to zero (0). <i>time</i> values can be 1 to 1440 minutes, or 1 to 24 hours. <i>Minutes Hours</i> value can be Minutes or Hours. <i>object</i> values can be: <ul style="list-style-type: none"> ACS Instance Device IP
Filter	
ACS Instance	Click Select to choose a valid ACS instance on which to configure your threshold.
Device IP	Click Select to choose or enter a valid device IP address on which to configure your threshold.
Protocol	Use the drop-down list box to configure the protocol that you want to use for your threshold. Valid options are: <ul style="list-style-type: none"> RADIUS TACACS+

Related Topics

- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Configuring General Threshold Information, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

External DB Unavailable

When ACS evaluates this threshold, it examines the RADIUS or TACACS+ failed authentications that have occurred during the specified interval up to the previous 24 hours.

From these failed authentications, ACS identifies those with the failure reason, External DB unavailable. Authentication records with this failure reason are grouped by a common attribute, such as ACS instance, user, and so on, and a count of the records within each of those groups is computed.

If the count of records for any group exceeds the specified threshold, an alarm is triggered. This can happen if, for example, you configure a threshold as follows:

External DB Unavailable count greater than 5 in the past one hour for a Device IP

If in the past hour, failed authentications with an External DB Unavailable failure reason have occurred for two different device IP addresses as shown in the following table, an alarm is triggered, because at least one device IP address has a count greater than 5.

Device IP	Count of External DB Unavailable Authentication Records
a.b.c.d	6
e.f.g.h	1

You can specify one or more filters to limit the failed authentications that are considered for threshold evaluation. Each filter is associated with a particular attribute in the records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on an external database that ACS is unable to connect to. Modify the fields in the **Criteria** tab as described in [Table 12-23](#).

Table 12-23 *External DB Unavailable*

Option	Description
External DB Unavailable	<p><i>percent count</i> greater than <i>num</i> in the past <i>time Minutes Hours</i> for a <i>object</i>, where:</p> <ul style="list-style-type: none"> Percent Count value can be Percent or Count. <i>num</i> values can be any one of the following: <ul style="list-style-type: none"> 0 to 99 for percent 0 to 99999 for count <i>time</i> values can be 1 to 1440 minutes, or 1 to 24 hours. Minutes Hours value can be Minutes or Hours. <i>object</i> values can be: <ul style="list-style-type: none"> ACS Instance Identity Store
Filter	
ACS Instance	Click Select to choose a valid ACS instance on which to configure your threshold.
Identity Group	Click Select to choose a valid identity group name on which to configure your threshold.
Identity Store	Click Select to choose a valid identity store name on which to configure your threshold.
Access Service	Click Select to choose a valid access service name on which to configure your threshold.
Protocol	<p>Use the drop-down list box to configure the protocol that you want to use for your threshold. Valid options are:</p> <ul style="list-style-type: none"> RADIUS TACACS+

Related Topics

- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Configuring General Threshold Information, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

RBACL Drops

When ACS evaluates this threshold, it examines Cisco Security Group Access RBACL drops that occurred during the specified interval up to the previous 24 hours. The RBACL drop records are grouped by a particular common attribute, such as NAD, SGT, and so on.

A count of such records within each of those groups is computed. If the count for any group exceeds the specified threshold, an alarm is triggered. For example, consider the following threshold configuration:

RBACL Drops greater than 10 in the past 4 hours by a SGT.

If, in the past four hours, RBACL drops have occurred for two different source group tags as shown in the following table, an alarm is triggered, because at least one SGT has a count greater than 10.

SGT	Count of RBACL Drops
1	17
3	14

You can specify one or more filters to limit the RBACL drop records that are considered for threshold evaluation. Each filter is associated with a particular attribute in the RBACL drop records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Modify the fields in the **Criteria** tab as described in [Table 12-24](#).

Table 12-24 *RBACL Drops*

Option	Description
RBACL drops	<p>greater than <i>num</i> in the past <i>time Minutes Hours</i> by a <i>object</i>, where:</p> <ul style="list-style-type: none"> <i>num</i> values can be any five-digit number greater than or equal to zero (0). <i>time</i> values can be 1 to 1440 minutes, or 1 to 24 hours. Minutes Hours value can be Minutes or Hours. <i>object</i> values can be: <ul style="list-style-type: none"> NAD SGT DGT DST_IP
Filter	
Device IP	Click Select to choose or enter a valid device IP address on which to configure your threshold.
SGT	Click Select to choose or enter a valid source group tag on which to configure your threshold.
DGT	Click Select to choose or enter a valid destination group tag on which to configure your threshold.
Destination IP	Click Select to choose or enter a valid destination IP address on which to configure your threshold.

Related Topics

- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Configuring General Threshold Information, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

NAD-Reported AAA Downtime

When ACS evaluates this threshold, it examines the NAD-reported AAA down events that occurred during the specified interval up to the previous 24 hours. The AAA down records are grouped by a particular common attribute, such as device IP address or device group, and a count of records within each of those groups is computed.

If the count for any group exceeds the specified threshold, an alarm is triggered. For example, consider the following threshold configuration:

AAA Down count greater than 10 in the past 4 hours by a Device IP

If, in the past four hours, NAD-reported AAA down events have occurred for three different device IP addresses as shown in the following table, an alarm is triggered, because at least one device IP address has a count greater than 10.

Device IP	Count of NAD-Reported AAA Down Events
a.b.c.d	15
e.f.g.h	3
i.j.k.l	9

You can specify one or more filters to limit the AAA down records that are considered for threshold evaluation. Each filter is associated with a particular attribute in the AAA down records and only those records that match the filter condition are counted. If you specify multiple filter values, only the records that match all the filter conditions are counted.

Choose this category to define threshold criteria based on the AAA downtime that a network access device reports. Modify the fields in the **Criteria** tab as described in [Table 12-25](#).

Table 12-25 NAD-Reported AAA Downtime

Option	Description
AAA down	<p>greater than <i>num</i> in the past <i>time</i> <i>Minutes\Hours</i> by a <i>object</i>, where:</p> <ul style="list-style-type: none"> <i>num</i> values can be any five-digit number greater than or equal to zero (0). <i>time</i> values can be 1 to 1440 minutes, or 1 to 24 hours. <i>Minutes\Hours</i> value can be Minutes or Hours. <i>object</i> values can be: <ul style="list-style-type: none"> Device IP Device Group

Table 12-25 NAD-Reported AAA Downtime (continued)

Option	Description
Filter	
ACS Instance	Click Select to choose a valid ACS instance on which to configure your threshold.
Device IP	Click Select to choose or enter a valid device IP address on which to configure your threshold.
Device Group	Click Select to choose a valid device group name on which to configure your threshold.

Related Topics

- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Configuring General Threshold Information, page 12-16](#)
- [Configuring Threshold Notifications, page 12-35](#)

Configuring Threshold Notifications

Use this page to configure alarm threshold notifications.

-
- Step 1** Select **Monitoring and Reports > Alarms > Thresholds**, then do one of the following:
- Click **Create** to create a new alarm threshold.
 - Click the name of an alarm threshold, or check the check box an existing alarm threshold and click **Edit** to edit a selected alarm threshold.
 - Click the name of an alarm threshold, or check the check box an existing alarm threshold and click **Duplicate** to duplicate a selected alarm threshold.
- Step 2** Click the **Notifications** tab.
- The Thresholds: Notifications page appears as described in [Table 12-26](#):

Table 12-26 Thresholds: Notifications Page

Option	Description
Severity	Use the drop-down list box to select the severity level for your alarm threshold. Valid options are: <ul style="list-style-type: none"> • Critical • Warning • Info
Send Duplicate Notifications	Check the check box to be notified of duplicate alarms. An alarm is considered a duplicate if a previously generated alarm for the same threshold occurred within the time window specified for the current alarm.

Table 12-26 *Thresholds: Notifications Page (continued)*

Option	Description
Email Notification	
Email Notification User List	<p>Enter a comma-separated list of e-mail addresses or ACS administrator names or both. Do one of the following:</p> <ul style="list-style-type: none"> Enter the e-mail addresses. Click Select to enter valid ACS administrator names. The associated administrator is notified by e-mail only if there is an e-mail identification specified in the administrator configuration. See Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-8 for more information. <p>When a threshold alarm occurs, an e-mail is sent to all the recipients in the Email Notification User List.</p> <p>Click Clear to clear this field.</p>
Email in HTML Format	Check this check box to send e-mail notifications in HTML format. Uncheck this check box to send e-mail notifications as plain text.
Custom Text	Enter custom text messages that you want associated with your alarm threshold.
Syslog Notification	
Send Syslog Message	<p>Check this check box to send a syslog message for each system alarm that ACS generates.</p> <p>Note For ACS to send syslog messages successfully, you must configure Alarm Syslog Targets, which are syslog message destinations. Understanding Alarm Syslog Targets, page 12-38 for more information.</p>

Related Topics

- [Viewing and Editing Alarms in Your Inbox, page 12-3](#)
- [Creating, Editing, and Duplicating Alarm Thresholds, page 12-11](#)
- [Deleting Alarm Thresholds, page 12-36](#)

Deleting Alarm Thresholds

To delete an alarm threshold:

-
- Step 1** Select **Monitoring and Reports > Alarms > Thresholds**.
The Alarms Thresholds page appears.
- Step 2** Check one or more check boxes the thresholds you want to delete, and click **Delete**.
- Step 3** Click **OK** to confirm that you want to delete the selected alarm(s).
The Alarms Thresholds page appears without the deleted threshold.
-

Configuring System Alarm Settings

System alarms are used to notify users of:

- Errors that are encountered by the Monitoring and Reporting services
- Information on data purging

Use this page to enable system alarms and to specify where alarm notifications are sent. When you enable system alarms, they are sent to the Alarms Inbox. In addition, you can choose to send alarm notifications through e-mail to select recipients and as syslog messages to the destinations specified as alarm syslog targets.

From the Monitoring and Report Viewer, choose **Monitoring Configuration > System Configuration > System Alarm Settings**.

Table 12-27 System Alarm Settings Page

Option	Description
System Alarm Settings	
Notify System Alarms	Check this check box to enable system alarm notification.
System Alarms Suppress Duplicates	Use the drop-down list box to designate the number of hours that you want to suppress duplicate system alarms from being sent to the Email Notification User List. Valid options are 1, 2, 4, 6, 8, 12, and 24.
Email Notification	
Email Notification User List	<p>Enter a comma-separated list of e-mail addresses or ACS administrator names or both. Do one of the following:</p> <ul style="list-style-type: none"> • Enter the e-mail addresses. • Click Select to enter valid ACS administrator names. The associated administrator is notified by e-mail only if there is an e-mail identification specified in the administrator configuration. See Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-8 for more information. <p>When a system alarm occurs, an e-mail is sent to all the recipients in the Email Notification User List.</p> <p>Click Clear to clear this field.</p>
Email in HTML Format	Check this check box to send e-mail notifications in HTML format. Uncheck this check box to send e-mail notifications as plain text.
Syslog Notification	
Send Syslog Message	<p>Check this check box to send a syslog message for each system alarm that ACS generates.</p> <p>For ACS to send syslog messages successfully, you must configure Alarm Syslog Targets, which are syslog message destinations. Understanding Alarm Syslog Targets, page 12-38 for more information.</p>

This section contains the following topics:

- [Creating and Editing Alarm Syslog Targets, page 12-38](#)
- [Deleting Alarm Syslog Targets, page 12-39](#)

Understanding Alarm Syslog Targets

Alarm syslog targets are the destinations where alarm syslog messages are sent. The Monitoring and Report Viewer sends alarm notification in the form of syslog messages. You must configure a machine that runs a syslog server to receive these syslog messages.

To view a list of configured alarm syslog targets, choose **Monitoring Configuration > System Configuration > Alarm Syslog Targets**.

**Note**

You can configure a maximum of two syslog targets in the Monitoring and Report Viewer.

This section contains the following topics:

- [Creating and Editing Alarm Syslog Targets, page 12-38](#)
- [Deleting Alarm Syslog Targets, page 12-39](#)

Creating and Editing Alarm Syslog Targets

To create or edit an alarm syslog target:

Step 1 Choose **Monitoring Configuration > System Configuration > Alarm Syslog Targets**.

The Alarm Syslog Targets page appears.

Step 2 Do one of the following:

- Click **Create**.
- Check the check box the alarm syslog target that you want to edit, then click **Edit**.

The Alarm Syslog Targets Create or Edit page appears.

Step 3 Modify the fields described in [Table 12-28](#).

Table 12-28 *Alarm Syslog Targets Create or Edit Page*

Option	Description
Identification	
Name	Name of the alarm syslog target. The name can be 255 characters in length.
Description	(Optional) A brief description of the alarm that you want to create. The description can be up to 255 characters in length.
Configuration	
IP Address	IP address of the machine that receives the syslog message. This machine must have the syslog server running on it. We recommend that you use a Windows or a Linux machine to receive syslog messages.

Table 12-28 Alarm Syslog Targets Create or Edit Page

Option	Description
Use Advanced Syslog Options	
Port	Port in which the remote syslog server listens. By default, it is set to 514. Valid options are from 1 to 65535.
Facility Code	Syslog facility code to be used for logging. Valid options are Local0 through Local7.

Step 4 Click **Submit**.

Related Topics

- [Understanding Alarm Syslog Targets, page 12-38](#)
- [Deleting Alarm Syslog Targets, page 12-39](#)

Deleting Alarm Syslog Targets



Note You cannot delete the default *nonstop* schedule.

To delete an alarm syslog target:

Step 1 Choose **Monitoring Configuration > System Configuration > Alarm Syslog Targets**.

The Alarm Syslog Targets page appears.

Step 2 Check the check box the alarm syslog target that you want to delete, then click **Delete**.

The following message appears:

Do you want to delete the selected item(s)?

Step 3 Click **Yes**.

The Alarm Syslog Targets page appears without the deleted alarm syslog targets.



Managing Reports

The reports in Cisco Secure ACS, Release 5.8.1 are enhanced to have a new look and feel that is more simple and easy to use. The reports are grouped in to logical categories to provide information related to authentication, session traffic, device administration, ACS server configuration and administration, and troubleshooting. The enhanced dynamic export option allows you to export the selected reports to an excel spreadsheet as a comma-separated values (.csv) file. The enhanced scheduling service allows you to queue reports and receive notification when the reports are available.

ACS 5.8.1 uses the flex based web interface to display reports. The new reports web interface in ACS 5.8.1 generates the RADIUS and TACACS+ reports three to four times faster (on an average) than ACS 5.5 reports. The report names and their filters are displayed on the left-hand side and the reports are displayed on the right-hand side of the Reports web interface. The enhanced web interface help you to navigate through the reports easily and to have a better control over different types of reports from left-pane, than going to the right-pane and make selection. ACS 5.8.1 does not support the Interactive Viewer feature as a whole; however, the “show or hide columns” and “fixing columns” (constituents of Interactive Viewer feature) are supported. You can export the report to a comma separated values file, open the file using Microsoft Excel Spreadsheet or using any other supported tool, and use the excel options to perform the operation.

The Monitoring and Reports drawer appears in the ACS web interface and contains the Launch Monitoring and Report Viewer option. Click **Launch Monitoring and Report Viewer** to open the Monitoring and Reports Viewer in a new window, which contains the following drawers:

- Monitoring and Reports
- Monitoring Configuration. (See [15, page 15-1](#).)

The Monitoring and Reports drawer on the web interface contains the Reports option. Click **Reports** to open the Reports Viewer in a new window.

You can run reports from Reports Web interface from any of the following pages:

- Favorites—**Reports > Favorites**
- ACS Reports—**Reports > ACS Reports > <report_type>**
- Saved and Scheduled Reports—**Reports > Saved and Scheduled Reports**

The reports that reside in these pages can be:

- System reports—Preconfigured with the ACS software; you can view the list of system reports in the **Reports > ACS Reports** pages.
- Customized reports—System reports that you have configured and saved.

For easy access, you can add reports to your Favorites page, from where you can customize and run reports. You can customize the reports and save them to access them frequently and run the customized reports. The saved reports are displayed under the Saved and Scheduled Reports drawer. The ACS

Reports provide a rich set of reports on log, diagnostic, and troubleshooting data retrieved from the ACS servers in your deployment. You can view these reports as tables, graphs, or charts and drill down further for more granular data.

Further, ACS allows you to:

- Filter the data in your report based on your requirements
- Add the reports periodically or on demand to a comma separated values file and print it
- Add the report to your list of favorites, from where you can access them frequently
- Customize a report and save it.

This chapter covers the following topics:

- [ACS Reports, page 13-2](#)
- [Running Reports, page 13-3](#)
- [Reports Navigation, page 13-3](#)
- [Exporting Reports, page 13-8](#)
- [Saving and Scheduling Reports, page 13-9](#)
- [Favorite Reports, page 13-14](#)
- [Available Reports, page 13-15](#)
- [Available Filters, page 13-20](#)
- [Changing Authorization for RADIUS Active Sessions Dynamically, page 13-22](#)
- [Understanding Charts, page 13-25](#)

ACS Reports

The Monitoring and Reports Viewer offers you a powerful dashboard that you can use to monitor the health of all ACS servers in your deployment. The dashboard also provides information on network access patterns and trends in traffic that you can use to administer your network efficiently. The Monitoring and Report Viewer provides you real-time data and vital statistics that help you proactively manage your network and prevent any attacks.

The Monitoring and Report Viewer component of Cisco Secure ACS collects log and configuration data from various ACS servers in your deployment, aggregates it, and provides interactive reports that help you analyze the data. It also provides you integrated monitoring, reporting, and troubleshooting capabilities to efficiently manage your network and troubleshoot network-related problems.

ACS comes with a set of predefined reports that you can run to obtain meaningful information from the log and configuration data obtained from ACS servers. [Table 13-2](#) lists the reports that are available in ACS under various categories. The report names and its filters and displayed in the left-pane. You can add or remove filters and run a report. The generated report appears on the right-pane.

Related Topics

- [Running Reports, page 13-3](#)
- [Reports Navigation, page 13-3](#)
- [Available Reports, page 13-15](#)
- [Available Filters, page 13-20](#)
- [Saving and Scheduling Reports, page 13-9](#)

Running Reports

This section describes how to run reports using reports view:

-
- Step 1** Choose **Monitoring and Reports > Reports > ACS 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 that are case sensitive, of which some are mandatory and some are optional. See [Table 13-3](#) for list of available filters.
- You can add or remove filters from the **Filters** drop-down list:
- To add filters, select the required filters from the **Filters** drop-down list. You can find a green color tick mark appears near the filter name after you select it.
 - To remove filters, deselect the filters from the **Filters** drop-down list. The green color tick mark disappears after you deselect the filter name.
- Step 4** Click **OK**.
- Step 5** Enter an appropriate value for the filters.
- Step 6** Click **Run**.
- ACS displays the generated report on the right pane.
-

**Note**

ACS displays a maximum of 250 pages per report with 100 records per page for RADIUS and TACACS+ AAA reports. For other reports, ACS displays a maximum of 50 pages per report with 100 records per page.

**Note**

When you click a link from the reports on Reports web interface, ACS opens that link in a new window. In ACS, the aggregation happens at 00:05 hrs every day and the cross launches from ACS reports details page display only the reports that are aggregated before the aggregation time. The logs that are generated after aggregation are not displayed until the next aggregation is complete. This limitation is applicable only for the cross launches in the reports details web interface. However, the Reports web interface displays all the reports irrespective of the aggregation time.

Related Topics

- [Exporting Reports, page 13-8](#)
- [Saving Reports, page 13-9](#)
- [Favorite Reports, page 13-14](#)
- [Scheduling Reports, page 13-12](#)

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.

When you run a report in the Reports Viewer, you see the first page data. To view or work with data, you use tools that help you navigate the report.

In the Reports Viewer, you can navigate through a report by using the paging tool as displayed in [Figure 13-1](#). Using this tool, you can click an arrow to view the next and previous page in the report.

Figure 13-1 *Paging Tool*

Generated at 2014-08-25 15:22:13.325

Total Pages: 19 GoTo: Go Page << 1 2 ... >> Records 1 to 100

MAC/IP Address	Access Service	Authentication Method	Network Device
.dc 00-0C-29-7F-A0-8B	serviceADAR1	MSCHAPV2	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithAD	MSCHAPV2	TE_NAD_TE1

373664

The viewer also supports going to a specific page by typing a page number in **Go To** as displayed in [Figure 13-2](#), and click **Go** the field.

Figure 13-2 *Going to a Specific Page*

Generated at 2014-08-25 15:22:13.325

Total Pages: 19 GoTo: Go Page << 1 2 ... >> Records 1 to 100

MAC/IP Address	Access Service	Authentication Method	Network Device
.dc 00-0C-29-7F-A0-8B	serviceADAR1	MSCHAPV2	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithAD	MSCHAPV2	TE_NAD_TE1

373663

The viewer displays the total number of pages and the current page as displayed in [Figure 13-3](#), and click **Go** the field.

Figure 13-3 *Total Pages*

Generated at 2014-08-25 15:22:13.325

Total Pages: 19 GoTo: Go Page << 1 2 ... >> Records 1 to 100


MAC/IP Address	Access Service	Authentication Method	Network Device
.dc 00-0C-29-7F-A0-8B	serviceADAR1	MSCHAPV2	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithAD	MSCHAPV2	TE_NAD_TE1

373666

For every reports that are displayed on the reports viewer, you can add, remove, or fix columns from the list using the column settings option available just above the reports header on the right-hand side as displayed in [Figure 13-4](#).

Figure 13-4 Report Settings

Generated at 2014-08-25 15:22:13.325

Total Pages: 19 GoTo: Go Page << 1 2 ... >> Records 1 to 100 

MAC/IP Address	Access Service	Authentication Method	Network Device M
.dc 00-0C-29-7F-A0-8B	serviceADAR1	MSCHAPV2	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithAD	MSCHAPV2	TE_NAD_TE1

373665

You change the order in which the reports header appear in the reports table. To change the reports header order, you need to drag the column and drop it in the place required.

Related Topics

- [Show or Hide Columns in Reports Table, page 13-5](#)
- [Fixing Columns in Reports Table, page 13-6](#)

Show or Hide Columns in Reports Table

Reports Viewer provides an option to show a column from the available list or hide an existing column in the reports table using the column settings feature. You can click on the column settings icon to see the available list of column names. If you find a green color tick mark near a column name as displayed in [Figure 13-5](#), that means the column name is selected and the selected column names appear in the reports table. The column names that does not have a tick mark near them are not selected; thus it will not appear in the reports table. You can show or hide multiple columns together.

To show or hide columns in reports table.

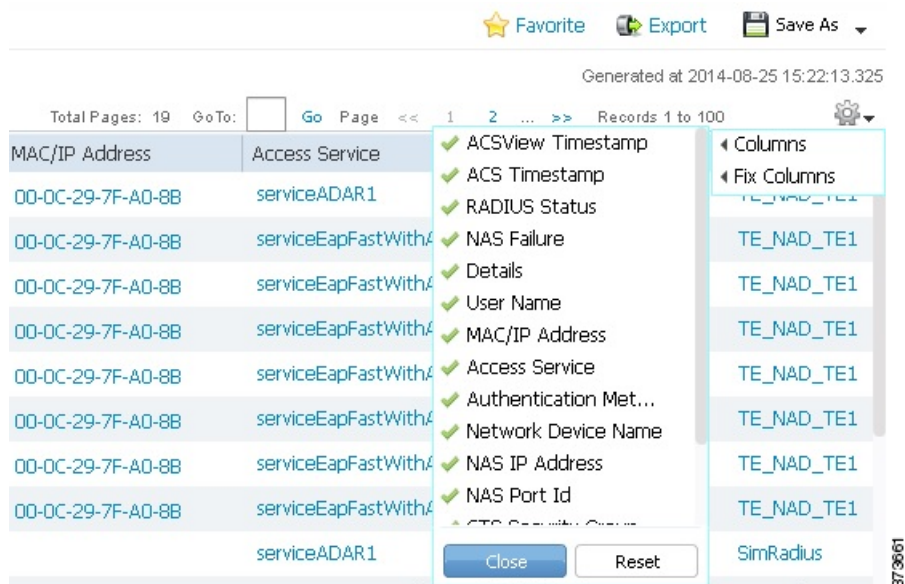
-
- Step 1** Choose **Monitoring and Reports > Reports > ACS Reports > report_type**.
- Step 2** Run a report, as described in [Running Reports, page 13-3](#).
- Step 3** Click the arrow the settings icon.
- Step 4** Click **Columns**.
- Step 5** Do one of the following:
- To show a column, select the column name from the drop-down list. A green color tick mark appears near the column name after you select it.
 - To hide a column, deselect the column name from the drop-down list. The green color tick mark disappears after you deselect the column name.
- Step 6** Click **Close**.
-



Note

You can click **Reset** to change the configuration to its default settings.

Figure 13-5 Show or Hide Columns



Fixing Columns in Reports Table

Reports Viewer provides an option to fix the reports header so that you cannot move that column inside the table as displayed in Figure 13-6. To fix columns in reports table.

- Step 1** Choose **Monitoring and Reports > Reports > ACS Reports > report_type**.
- Step 2** Run a report, as described in [Running Reports, page 13-3](#).
- Step 3** Click the arrow the settings icon.
- Step 4** Click **Fix Columns**.
- Step 5** Do one of the following:
 - To fix a column, select the column name from the drop-down list. A green color tick mark appears near the column name after you select it.
 - To remove a fixed column, deselect the column name from the drop-down list. The green color tick mark disappears after you deselect the column name.
- Step 6** Click **Close**.



Note

You can click **Reset** to change the configuration to its default settings.

Favorite
 Export
 Save As ▼

Generated at 2014-08-25 15:22:13.325

Total Pages: 19 GoTo: Go Page << 1 2 ... >> Records 1 to 100

MAC/IP Address	Access Service	Authentication Method	Columns
00-0C-29-7F-A0-8B	serviceADAR1	ACSView Timestamp	Fix Columns
00-0C-29-7F-A0-8B	serviceEapFastWithA	ACS Timestamp	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	RADIUS Status	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	NAS Failure	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	Details	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	User Name	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	MAC/IP Address	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	Access Service	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	Authentication Met...	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	Network Device Name	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	NAS IP Address	TE_NAD_TE1
00-0C-29-7F-A0-8B	serviceEapFastWithA	NAS Port Id	SimRadius
	serviceADAR1	CTC Call with Group	SimRadius
	serviceEapFastWithA		SimRadius
	serviceEapFastWithAD	PAP_ASCII	SimRadius

ACS 5.8.1 allows the user to sort data in the reports table based on the entries in the column either in ascending or descending order. You can click a column title once to sort the complete reports table based on the selected column entries in ascending order. You can find an upward-pointing arrow to the right of the column title indicating that the column entries are sorted in ascending order. You can click on a column title again to sort the table based on the selected column entries in descending order. You can find a downward-pointing arrow to the right of the column title indicating that the column entries are sorted in descending order.

ACS 5.8.1 allows the user to filter the data entries in reports table column-wise. ACS 5.8.1 uses the “contains” parameter to filter the data. The reports table has either a drop-down list or a text box each column heading except a few columns to which the filtering is not applicable. Click the drop-down list to view the available filtering options. You have to select the entry or multiple entries from the drop down list or enter the text in the text box to filter table entries.

Step 1 Choose **Monitoring and Reports** > **Reports** > **ACS Reports** > *report_type*.

Step 3 Perform one of the following actions:

- ## User Guide for Cisco Secure Access Control System 5.8.1

- If a column has a text box, then enter the filter text in the text box.

Step 4 Click **OK**.

The reports table is now filtered based on the selected column entries.

Exporting Reports

In ACS 5.8.1, you can export report data to an excel spreadsheet as a comma-separated values (.csv) file. Previous releases of ACS allowed you to export reports and copy the comma separated value file to the local file system. You need to copy the exported file using the **copy** command to a remote location. But in ACS 5.8.1, you have the option to configure the remote repository to which the exported reports are stored. After you export the data, you will receive an email detailing the location of the report. You can track the status of the records in the scheduler page.



Note

To receive a email notification for the exported reports, you need to configure the email server details on the Email Settings page. See [Specifying E Mail Settings, page 15-16](#) to configure email server details. You will not receive any email if you did not configure the email server details from Email Settings page.

Step 1 Select **Monitoring and Reports > Reports > ACS Reports > *report_type* >**, where *report_type* is the type of report.

The available reports for the report type you selected are displayed.

Step 2 Run a report, as described in [Running Reports, page 13-3](#).

Step 3 Click **Export**.

Step 4 Choose a repository from the drop-down list.

You cannot export the following reports:

- Authentication Summary
- Health Summary
- All Security Group Access reports except RBACL Drop Summary report
- Endpoint reports
- Network Device Session Status



Note

When you export an ACS Administrator Entitlement Summary Report to a remote repository, ACS 5.6 exports the two columns “Administrator” and “Roles” from the reports table to a comma separated values file (csv). But, ACS 5.8.1 exports the additional column “Resources and Privileges” along with the Administrator and Roles columns.

If you configure a new repository when you are generating reports from the reports web interface, the newly configured repository will not be available for exporting the generated reports. You need to close the reports web interface and open it again to view the newly configured repository to export the generated reports.

**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**

When you use Microsoft Excel to view the exported records, you should be aware of the worksheet size limitations. In Microsoft Excel 2007 and 2010, the maximum limit for a worksheet size is 1,048,576 rows by 16,384 columns. For more information, see: <http://office.microsoft.com/en-us/excel-help/excel-specifications-and-limits-HP010342495.aspx>.

Saving and Scheduling Reports

In ACS 5.8.1, you can save or schedule reports from the new Reports web interface. The Saved and Scheduled Reports section of the Reports web interface has the following options:

- [Saved Reports, page 13-9](#)
- [Scheduled Reports, page 13-11](#)

Saved Reports

This section contains the following topics:

- [Saving Reports, page 13-9](#)
- [Editing Saved Reports, page 13-10](#)
- [Deleting Saved Reports, page 13-10](#)

Saving Reports

You can customize a report and save the changes as a new report. The saved reports are displayed under Saved and Scheduled reports section of Reports web interface.

-
- Step 1** Run a report as described in [Running Reports, page 13-3](#).
- Step 2** Click **Save As** in the top right-hand corner of the report summary page.
- Step 3** Choose **Report**.
- Step 4** Enter the **Name** and **Description** in the dialog box.
- Step 5** Click **Save**.

The report is now saved along with the selected filter values.

**Note**

You can edit the report name and description of the saved reports. To edit the report name and description of the saved reports, select the report that you want to edit and click **Edit Setting**.

Editing Saved Reports

You can customize a report and save that as a new report in Saved reports page. The saved reports appear with the customized filters. You can add new filters or remove the existing filters, edit them, and save that as a new report. You can customize a saved report and save that report as a new report using the **Save As New** option.

-
- Step 1** Choose **Monitoring and Reports > Reports > Saved and Scheduled Reports > Saved Reports**.
- Step 2** Select the report that you want to edit.
- Step 3** The selected saved reports appear with the existing filters.
- Step 4** You can add or remove filters from the **Filters** drop-down list:
- To add filters, select the required filters from the **Filters** drop-down list. You can find a green color tick mark near the selected filters.
 - To remove filters, deselect the filters from the **Filters** drop-down list. The green color tick mark disappears after you deselect it.
- Step 5** Click **OK**.
- Selected filters appears under the saved reports with its default values.
- Step 6** Enter the required details for the selected filters and click **Run**.
- Step 7** Click **Save As** in the top right-hand corner of the report summary page.
- Step 8** Choose **Report**.
- Step 9** Enter the **Name** and **Description** in the dialog box.
- Step 10** Click **Save** to save the report or **Save As New** to save this report as a new report.
- If you click **Save**, ACS overrides the existing customization and save this report.
 - If you click **Save As New**, ACS do not override the existing customization. The edited report is now saved as a new report with the name specified.
-

Deleting Saved Reports

To delete a report from the Saved Reports page:

-
- Step 1** Choose **Monitoring and Reports > Reports > Saved and Scheduled Reports > Saved Reports**.
- Step 2** Select the report that you want to delete, and click **Delete**.
- Step 3** Click **OK** to confirm that you want to delete the selected saved report.
- The Saved Report is now deleted.
-

Related Topics

[Saving Reports, page 13-9](#)

Scheduled Reports

In ACS 5.8.1, you can schedule reports for a future date in such a way that ACS automatically generates the report. This can be done using the scheduled reports feature available in the Saved and Scheduled Reports drawer of Reports web interface.

In ACS 5.5, this feature is available only for the RADIUS authentication, RADIUS accounting, TACACS+ authentication, TACACS+ authorization, and TACACS+ accounting reports. But in ACS 5.8.1, this feature is available for all the ACS Reports other than a few reports listed below.

You cannot schedule the following reports in ACS 5.8.1:

- ACS Health Summary
- ACS Instance Authentication Summary
- Top N Authentication by ACS Instance
- AAA Down Summary
- Top N AAA Down By Network Device
- RBACL Drop Summary
- RADIUS Active Sessions
- RADIUS Session History
- RADIUS Terminated Sessions
- TACACS Active Sessions
- TACACS Session History
- TACACS Terminated Sessions

In ACS 5.8.1, you have the option to configure the remote repository to which the generated reports are exported and stored. ACS generates the scheduled reports based on the given time range, exports them to a comma separated values file, and stores them in the specified remote repository.

An email notification is sent whenever a scheduled report is generated successfully. To receive a email notification for the scheduled reports, you need to configure the email server details on the Email Settings page. See [Specifying E Mail Settings, page 15-16](#) to configure email server details. The email notification contains the following information:

- File Name—Name of the generated report file. The format of the filename is RptExp_<admin_name>_<scheduledreport_name>_<generated_on>_<randomnumber>.csv. For instance, if the name of the scheduled report is “report1”, then the filename is displayed as: RptExp_acsadmin_report1_2014-08-05_14-00-00.000000182.csv.
- Repository Name—Name of the remote repository where the generated reports are stored.
- Generated on—The date and time at which the report is generated.

ACS does not generate any alarms or email notifications if a scheduled report generation fails. To know the status of the scheduled reports, go to the **Monitoring Configuration > System Operations > Scheduler** page and check for the status.

This section contains the following topics:

- [Scheduling Reports, page 13-12](#)
- [Deleting Scheduled Reports, page 13-13](#)

**Note**

When you upgrade from ACS 5.5 to 5.8.1, the existing Scheduled Reports in ACS 5.5 will be displayed under **Saved and Scheduled Reports > Scheduled Reports** Page in ACS 5.8.1.

Scheduling Reports

To schedule ACS reports:

- Step 1** Choose **Monitoring and Reports > Reports > Saved and Scheduled Reports > Scheduled Reports**.
- Step 2** Run the report as described in [Running Reports, page 13-3](#).
- Step 3** Click **Save As** in the top right-hand corner of the report summary page.
- Step 4** Choose **Scheduled Report**.

The Scheduled Reports properties page appears. Complete the fields in the Scheduled Reports page as described [Table 13-1](#).

Table 13-1 *Scheduled Reports Properties Page*

Option	Description
Identification	
Name	(Required) Name of the scheduled report.
Description	(Optional) A brief description of the scheduled report.
Repository	(Required) Select a remote repository from the drop-down list to export and store in it. You need to configure the remote repositories using the ACS CLI interface or the ACS web interface.
Send Email Notification	<p>(Required) Enter the email address to which an email notification or alarm should be sent upon successful generation of the scheduled report. You can add multiple email addresses separating them with a comma.</p> <p>You will not receive an email for the scheduled reports if you do not configure the email server details on the Email Settings page. To configure email server details, see Specifying E Mail Settings, page 15-16.</p>
Schedule	
Frequency	<p>(Required) Select the frequency of the scheduled report from the drop-down list. The available frequencies are One Time, hourly, daily, weekly, and monthly.</p> <ul style="list-style-type: none"> • One Time—ACS generates the report only once based on the schedule. • Hourly—ACS generates the report on an hourly basis for the specified time period. • Daily—ACS generates the report every day at the specified time. • Weekly—ACS generates the report on the specified day or days of every week. You must configure the day or days in the Day option. • Monthly—ACS generates the report on the specified day or days of every month. You must configure the day or days in Day option. • Yearly—ACS generates the report on the specified day of the selected month. You must configure the day, month, and time.

Table 13-1 Scheduled Reports Properties Page (continued)

Option	Description
At Time	(Required) Select the hour and minutes of the day at which the report should be triggered. The time ranges between 12:00 AM and 11:30 PM. For example, if you select 6:30 AM, the report is generated at 6:30 a.m. for the specified time period.
Every	(Optional) Select the hour (<i>n</i>) of the day from the drop-down list to run the report for every <i>n</i> hour on that day between the configured time interval. In addition, select the time range from the drop-down list for which you want ACS to generate the report between <i>x</i> and <i>y</i> hours. For example, if you select 3 hours and run between 8 AM and 5 PM, then the report runs for every three hours between 8 AM and 5 PM. This option appears only when you select the frequency as hourly.
Month	(Optional) Select the month on which you want to run your report. This option appears only when you select the frequency as Monthly.
On Day	<p>(Optional) Check the check boxes the days or select the day from the drop-down list on which to generate the reports. This option over rules the Frequency sometimes.</p> <p>For example, if you select the frequency as daily and select the days Monday, Tuesday, and Thursday; the reports are generated only for the selected days and not daily.</p> <p>When you set the frequency as hourly, daily, or weekly, this option displays the check boxes from Monday to Sunday. You need to check the appropriate check box or boxes the days.</p> <p>When you set the frequency as monthly or yearly, this option displays the a drop-down list that ranging from day 1 through 31 and last day. You need to select day from the drop-down list. For example, if you select 5 from the drop-down list, the reports run on 5th day of every month.</p>
Start Date	(Optional) Click the icon the Start Date field to select a date from when you want ACS to start generating the scheduled reports. The date format is YYYY/MM/DD.
End Date	(Optional) Click the icon the End Date field to select a date on which you want ACS to stop generating the scheduled reports. The date format is YYYY/MM/DD.

Step 5 Click **Save**.

The scheduled report is saved.

Deleting Scheduled Reports

To delete a report from the Scheduled Reports page:

Step 1 Choose **Monitoring and Reports > Reports > Saved and Scheduled Reports > Scheduled Reports**.

Step 2 Select the report that you want to delete, and click **Delete**.

Step 3 Click **OK** to confirm that you want to delete the selected report.

The Scheduled Report is now deleted.

Favorite Reports

You can add reports that you most frequently use to your Favorites page so that you do not have to navigate each time to get to your favorite report. In ACS 5.5, you can customize the catalog reports (ACS reports in ACS 5.8.1) and add them to favorite reports along with the customized parameters so that you can run the customized report from favorite reports section next time. But in ACS 5.8.1, the favorite reports provide the same functionality of ACS reports.

When you upgrade from ACS 5.5, 5.6, or 5.7 to 5.8.1, the existing favorite reports in ACS 5.5, 5.6, or 5.7 will be displayed under Saved reports section in ACS 5.8.1. The favorite reports section in ACS 5.8.1 displays the following default favorite reports:

- ACS Configuration Audit
- ACS System Diagnostics
- RADIUS Authentication
- TACACS Authentication

This section contains the following topics:

- [Adding Favorite Reports, page 13-14](#)
- [Deleting Reports from Favorites, page 13-14](#)

Adding 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.

To add a report to your Favorites page:

Step 1 Select **Monitoring and Reports > Reports > ACS Reports > *report_type* >**, where *report_type* is the type of report.

The available reports for the report type you selected are displayed.

Step 2 Run a report, as described in [Running Reports, page 13-3](#).

Step 3 Click **Favorite in the top right-hand corner of the report summary page**.

The report appears in your Favorites list.

Deleting Reports from Favorites

To delete a report from the Favorites page:

Step 1 Select **Monitoring and Reports > Reports > Favorites**.

Step 2 Select the report that you want to delete from favorites, and click **Unfavorite** in the top right-hand corner of the report summary page.

The selected report disappears from the Favorites section.



Note

Favorite Reports in ACS may disappear from the Reports web interface after every database purge activity. This issue occurs when the report is created by an external identity store user. At the time of database purge activity, ACS verifies the internal user database to check if the user who created the favorite reports is available in the internal identity store users list. If the user is not available in the internal identity store user list, ACS deletes that report from the Reports web interface. The workaround for this issue is to create a local ACS administrator with the same name as the external identity store user, so that the favorite reports will not be deleted after every database purge activity.



Note

When you delete a system report from the Favorites page, the system report is not displayed in the favorites page. The system report will not be deleted from the **ACS Reports** section.



Note

The shared reports that were created in ACS 5.5, 5.6, or 5.7 are deleted after you upgrade to ACS 5.8.1.

Available Reports

[Table 13-2](#) lists the preconfigured reports, grouped according to their category. Descriptions of the report functionality and logging category are also provided. These reports are available when you select Monitoring and Reports, launch Monitoring and Report Viewer, and then select **Monitoring and Reports > Reports > ACS Reports**.

Table 13-2 Available Reports

Report Name	Description	Logging Category
AAA Protocol		
AAA diagnostics	Provides AAA diagnostic details based on severity for a selected time period.	Policy diagnostics, identity stores diagnostics, authentication flow diagnostics, RADIUS diagnostics, TACACS+ diagnostics
Authentication Trend	Provides RADIUS and TACACS+ authentication summary information for a selected time period; along with a graphical representation.	Passed authentications, failed attempts
RADIUS Accounting	Provides user accounting information based on RADIUS for a selected time period.	RADIUS accounting
RADIUS Authentication	Provides RADIUS authentication details for a selected time period.	Passed authentications, failed attempts
TACACS Accounting	Provides user or command accounting information for TACACS+ authentications for a selected time period.	TACACS+ accounting
TACACS Authentication	Provides TACACS+ authentication details for a selected time period.	Passed authentications, failed attempts

Table 13-2 Available Reports (continued)

Report Name	Description	Logging Category
TACACS Authorization	Provides TACACS+ authorization details for a selected time period.	Passed authentications, failed attempts
Access Service		
Access Service Authentication Summary	Provides RADIUS and TACACS+ authentication summary information for a particular access service for a selected time period; along with a graphical representation.	Passed authentications, failed attempts
Top N Authentications By Access Service	Provides the top N passed, failed, and total authentication count for RADIUS and TACACS+ authentications with respect to the access service for a selected time period.	Passed authentications, failed attempts
ACS Instance		
ACS Administrator Entitlement	Shows the role of the administrator in ACS and the: <ul style="list-style-type: none"> Tasks in ACS that the administrator is entitled to access Privileges that the administrator has for each of those operations 	None
ACS Administrator Logins	Provides access-related events for administrators that includes login, logout, events, and reasons for failed login attempts.	Administrative and operational audit
ACS Configuration Audit	Provides all the configuration changes done in ACS by the administrator for a selected time period.	Administrative and operational audit
ACS Health Summary	Provides the CPU, memory utilization, RADIUS and TACACS+ latency and throughput (in tabular and graphical formats). It also gives process status, process downtime, and disk space utilization for a particular ACS instance in a selected time period.	System statistics
ACS Instance Authentication Summary	Provides RADIUS and TACACS+ authentication summary information for a particular ACS instance for a selected time period; along with a graphical representation. This report could take several minutes to run depending on the number of records in the database. When you reload this report, if rate of incoming syslog messages is around 150 messages per second or more, the total number of passed and failed authentications that appear above the graph and the passed and failed authentication count that is displayed in the table do not match.	Passed authentications, failed attempts
ACS Log Information	Provides ACS log information for a particular log category and ACS server for a selected time period.	All log categories

Table 13-2 Available Reports (continued)

Report Name	Description	Logging Category
ACS Operations Audit	Provides all the operational changes done in ACS by the administrator for a selected time period.	Administrative and operational audit
ACS System Diagnostics	Provides system diagnostic details based on severity for a selected time period.	Internal Operations Diagnostics, distributed management, administrator authentication and authorization
Top N Authentication by ACS Instance	Provides the top N passed, failed, and total authentication count for RADIUS and TACACS+ protocol with respect to a particular ACS instance for a selected time period.	Passed authentications, failed attempts
User Change Password Audit	Provides the username of the internal user, identity store name, name of the ACS instance, and time when the user password was changed. Helps to keep track of all changes made to internal user passwords across all ACS interfaces.	Administrative and operational audit
AD Connector Operations	Provides background operations performed by AD connector, such as ACS 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.	
Endpoint		
Endpoint MAC Authentication Summary	Provides the RADIUS authentication summary information for a particular MAC or MAB for a selected time period; along with a graphical representation.	Passed authentications, failed attempts
Top N Authentications By Endpoint MAC Address	Provides the top N passed, failed, and total authentication count for RADIUS protocol with respect to MAC or MAB address for a selected time period.	Passed authentications, failed attempts
Top N Authentications By Machine	Provides the top N passed, failed, and total authentication count for RADIUS protocol with respect to machine information for a selected time period.	Passed authentications, failed attempts
Failure Reason		
Authentication Failure Code Lookup	Provides the description and the appropriate resolution steps for a particular failure reason.	N/A
Failure Reason Authentication Summary	Provides the RADIUS and TACACS+ authentication summary information for a particular failure reason; along with a graphical representation for a selected time period.	Failed attempts
Top N Authentications By Failure Reason	Provides the top N failed authentication count for RADIUS and TACACS+ protocols with respect to Failure Reason for a selected time period.	Failed attempts

Table 13-2 Available Reports (continued)

Report Name	Description	Logging Category
Network Device		
AAA Down Summary	Provides the number of AAA unreachable events that a NAD logs within a selected time period.	N/A
Network Device Authentication Summary	Provides the RADIUS and TACACS+ authentication summary information for a particular network device for a selected time period, along with the graphical representation.	Passed authentications, failed attempts
Network Device Log Messages	Provides you the log information of a particular network device, for a specified time period.	N/A
Session Status Summary	Provides the port sessions and status of a particular network device obtained by SNMP. This report uses either the community string provided in the report or the community string configured in the web interface Monitoring And Reports -> Launch Monitoring And Report Viewer -> Monitoring Configuration -> SNMP Settings .	N/A
Top N AAA Down By Network Device	Provides the number of AAA down events encountered by each of the network devices.	N/A
Top N Authentications by Network Device	Provides the top N passed, failed, and total authentication count for RADIUS and TACACS+ protocols with respect to network device for a selected time period.	Passed authentications, failed attempts
Security Group Access		
RBACL Drop Summary	Provides a summary of RBACL drop events for a selected time period.	N/A
SGT Assignment Summary	Provides a summary of SGT assignments for a selected time period.	Passed authentications
Top N RBACL Drops By Destination	Provides the top N RBACL drop event count with respect to destination for a selected time period.	N/A
Top N RBACL Drops By User	Provides the top N RBACL drop event count with respect to the user for a selected time period.	N/A
Top N SGT Assignments	Provides the top N SGT assignment count for a selected time period.	Passed authentications
Session Directory		

Table 13-2 Available Reports (continued)

Report Name	Description	Logging Category
RADIUS Active Sessions	Provides information on RADIUS authenticated, authorized, and started sessions. RADIUS Active Sessions report allows you to dynamically control active RADIUS sessions. With this feature, you can send a reauthenticate or disconnect request to a NAD to: <ul style="list-style-type: none"> • Reauthenticate the user • Terminate the session • Terminate the session and restart the port • Terminate the session and shut down the port 	Passed authentications, RADIUS accounting
RADIUS Session History	Provides a summary of RADIUS session history, such as total authenticated, active, and terminated sessions and total and average session duration and throughput for a selected time period.	Passed authentications, RADIUS accounting
RADIUS Terminated Sessions	Provides all the RADIUS terminated session information for a selected time period.	Passed authentications, RADIUS accounting
TACACS Active Sessions	Provides information on TACACS+ active sessions.	TACACS+ accounting
TACACS Session History	Provides TACACS+ session history summary, such as total active and terminated sessions and total and average session duration and throughput for a selected time period.	TACACS+ accounting
TACACS Terminated Sessions	Provides TACACS terminated session details for a selected time period.	TACACS+ accounting
User		
Top N Authentications By User	Provides top N passed, failed, and total authentication count for RADIUS and TACACS+ protocol with respect to users for a selected time period.	Passed authentications, failed attempts
User Authentication Summary	Provides RADIUS and TACACS+ authentication summary information for a particular user for a selected time period; along with the graphical representation.	Passed authentications, failed attempts

**Note**

ACS 5.8.1 displays a detailed audit reports on ACS configuration audit reports page for creating, editing, or re-ordering access service policies from the ACS web interface.

**Note**

ACS displays the current day report for the summary reports having hyperlinks. To generate report for an older date or a time range, you must run a manual report for the user.

Available Filters

ACS 5.8.1 provides you an option to select the filter values from the available values for all the filters. You have to enter the first three letters of the filter values in the filter fields. ACS displays the available values after entering the first three letters.


Note

Not all options listed in [Table 13-3](#) are used in selecting data for all reports.

Table 13-3 *Available Filters*

Option	Description
User	Enter a valid username on which to configure your threshold.
MAC Address	Enter a valid MAC address on which to run your report.
Identity Group	Enter a valid identity group name on which to run your report.
Device Name	Enter a valid device name on which to run your report.
Device IP	Enter a valid device IP address on which to run your report.
SNMP Community	Configure SNMP preferences to authenticate access to MIB objects. For more information, see Configuring SNMP Preferences, page 15-19 . This community string is used by ACS to query information using SNMP on AAA client, and cannot be used by SNMP manager to query MIB information on ACS.
Device Group	Enter a valid device group name on which to run your report.
Access Service	Enter a valid access service name on which to run your report.
Identity Store	Enter a valid identity store name on which to run your report.
ACS Instance	Enter an valid ACS instance name on which to run your report.
Failure Reason	Enter a valid failure reason name on which to run your report.
Protocol	Use the drop down list box to select which protocol on which you want to run your report. Valid options are: <ul style="list-style-type: none"> • RADIUS • TACACS+
Authentication Status	Use the drop down list box to select which authentication status on which you want to run your report. Valid options are: <ul style="list-style-type: none"> • Pass Or Fail • Pass • Fail
Radius Audit Session ID	Enter the RADIUS audit session identification name on which you want to run a report.
ACS Session ID	Enter the ACS session identification name on which you want to run a report.

Table 13-3 Available Filters (continued)

Option	Description
Severity	Use the drop down list box to select the severity level on which you want to run a report. This setting captures the indicated severity level and those that are higher within the threshold. Valid options are: <ul style="list-style-type: none"> • Fatal • Error • Warning • Info • Debug
End Point IP Address	Enter the end point IP address on which you want to run a report.
Command Accounting Only	Check the check box to enable your report to run for command accounting.
Top	Use the drop down list box to select the number of top (most frequent) authentications by access service on which you want to run your report. Valid options are: <ul style="list-style-type: none"> • 10 • 50 • 100 • 500 • 1000 • 5000
By	Use the drop down list box to select the type of authentications on which you want to run your report. Valid options are: <ul style="list-style-type: none"> • Passed Authentications • Failed Authentications • Total Authentications
Administrator Name	Enter the administrator username for which you want to run your report.
Object Type	Enter a valid object type on which you want to run your report.
Object Name	Enter the name of the object on which you want to run your report.
Authorization Status	Use the drop down list box to select which authentication status on which you want to run your report. Valid options are: <ul style="list-style-type: none"> • Pass Or Fail • Pass • Fail

Table 13-3 Available Filters (continued)

Option	Description
Time Range	<p>Use the drop down list box to select the time range on which you want to run your report. Valid options are:</p> <ul style="list-style-type: none"> • Last 30 Minutes (for AAA Protocol reports and ACS Health Summary report only) • Last Hour (for AAA Protocol reports and ACS Health Summary report only) • Last 12 Hours (for AAA Protocol reports and ACS Health Summary report only) • Today • Yesterday • Last 7 Days • Last 30 Days • Custom—You must configure a Start Date and End Date, or a Day. <p>Note Some options are not valid for some Time Range entries of the various reports.</p>
Start Date	Enter a date, or click the date selector icon to enter the start date for which you want run your report.
End Date	Enter a date, or click the date selector icon to enter the end date for which you want run your report.
Start Time	Enter the start time you want to run the report.
End Time	Enter the end time you want to run the report.
Day	Enter a date, or click the date selector icon to enter the end date for which you want run your report.
Run	Click to run the report for which you have made selections.

Related Topics

- [ACS Reports, page 13-2](#)
- [Favorite Reports, page 13-14](#)
- [Available Reports, page 13-15](#)
- [Running Reports, page 13-3](#)

Changing Authorization for RADIUS Active Sessions Dynamically

ACS provides the Dynamic Change of Authorization (CoA) feature through a new report, the RADIUS Active Sessions report, which allows you to dynamically control active RADIUS sessions. With this feature, you can send a reauthenticate or disconnect request to a NAD to:

- Troubleshoot issues related to authentication—You can use the Disconnect:None option to follow up with an attempt to reauthenticate again.
You must not use the disconnect option to restrict access. To restrict access, use the shutdown option.
- Block a problematic host—You can use the Disconnect:Port Disable option to block an infected host that sends a lot of traffic over the network.

The RADIUS protocol currently does not support a method for re-enabling a port that is shut down.

- Force endpoints to reacquire IP addresses—You can use the Disconnect:Port Bounce option for endpoints that do not have a supplicant or client to generate a DHCP request after VLAN change.
- Push an updated authorization policy to an endpoint—You can use the Re-Auth option to enforce an updated policy configuration, such as a change in the authorization policy on existing sessions based on the administrator's discretion.

For example, if posture validation is enabled, when an endpoint gains access initially, it is usually quarantined. After the endpoint's identity and posture are known, it is possible to send the CoA Re-Auth command to the endpoint for the endpoint to acquire the actual authorization policy based on its posture.

Legacy NAS devices do not support the CoA feature. Cisco plans to support CoA in all its devices as part of the NPF program.

**Note**

For the CoA commands to be understood correctly by the device, it is important that you configure the options appropriately.

For the CoA feature to work properly, you must configure in ACS the shared secret of each and every device for which you want to dynamically change the authorization. ACS uses the shared secret configuration, both for requesting access from the device and for issuing CoA commands to it.

This section contains the following topics:

- [Enabling RADIUS CoA Options on a Device, page 13-23](#)
- [Changing Authorization and Disconnecting Active RADIUS Sessions, page 13-24](#)

Enabling RADIUS CoA Options on a Device

To view all the RADIUS Active Session reports you have to enable RADIUS CoA options on the device.

To configure the RADIUS CoA options:

Step 1 Configure MAB, 802.1X and Web Authentication on the NAD against ACS RADIUS Server.

Step 2 Configure CoA on the NAD as follows, which is connected to the supplicant.

```
aa server radius dynamic-author
client {<ip_addr> - <name>} [vrf <vrfname>] [server-key<string>]
server-key [0 - 7] <string>
port <port-num>
auth-type {any - all - session-key}
ignore session-key
ignore server-key
```

Step 3 Configure the authentication order.

Changing Authorization and Disconnecting Active RADIUS Sessions



Note

Some of the NADs in your deployment do not send an Accounting Stop or Accounting Off packet after a reload. As a result of this, you might find two sessions in the Session Directory reports, one of which has expired. Hence, when you want to dynamically change the authorization of an active RADIUS session or disconnect an active RADIUS session, ensure that you always choose the most recent session.

To change authorization or disconnect an active RADIUS session:

Step 1 Run the RADIUS Active Sessions report under Session Directory.

See [Running Reports, page 13-3](#) for information on how to run a RADIUS Active Sessions report.

A report similar to the one shown in [Table 13-3](#) appears.

Figure 13-7 RADIUS Active Session Report

Initiated	Updated	Dur	Packets In	Packets Out	User Name	Radius User Name	CTS Security Group	Framed IP	Session	CoA	ACS Server	Audit Session	Acct Session Id	Calling Station ID	NA
2014-09-04 1	2014-09-0 88	0	0	0	testuser	testuser			Started		acs68		123	1.1.1.4	10
2014-09-04 1	2014-09-0 128	0	0	0	sarathi	sarathi			Started		acs68		123	1.1.1.4	10
2014-09-04 1	2014-09-0 132	0	0	0	sarathi	sarathi			Authenticated		acs68			1.1.1.4	10
2014-09-04 1	2014-09-0 169	0	0	0	sarathi	sarathi			Authenticated		acs68			1.1.1.4	10

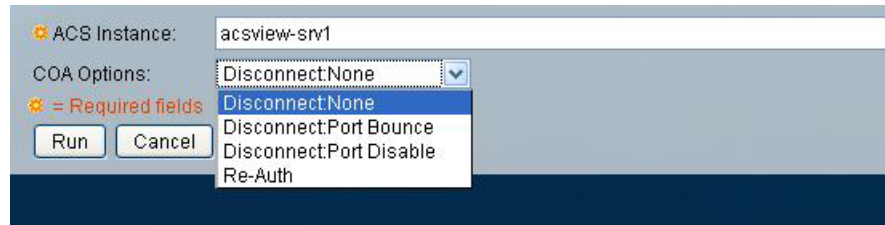
Step 2 Click the CoA link from the RADIUS session that you want to reauthenticate or terminate.

The Change of Authorization Request page appears.

Step 3 Select a CoA option from the CoA option drop-down list box shown in [Figure 13-8](#).

Valid options are:

- Disconnect:None—Do not terminate the session.
- Disconnect:Port Bounce—Terminate the session and restart the port.
- Disconnect:Port Disable—Terminate the session and shut down the port.
- Re-Auth—Reauthenticate the user.

Figure 13-8 CoA Options

Step 4 Click **Run** to reauthenticate or disconnect the RADIUS session.

If your change of authorization fails, it might be because of any of the following reasons:

- Device does not support CoA
- Changes to the identity or authorization policy
- Shared secret mismatch

Step 5 See the [Troubleshooting RADIUS Authentications, page 14-6](#) to troubleshoot a failed change of authorization attempt.

A failed dynamic CoA will be listed under failed RADIUS authentications.

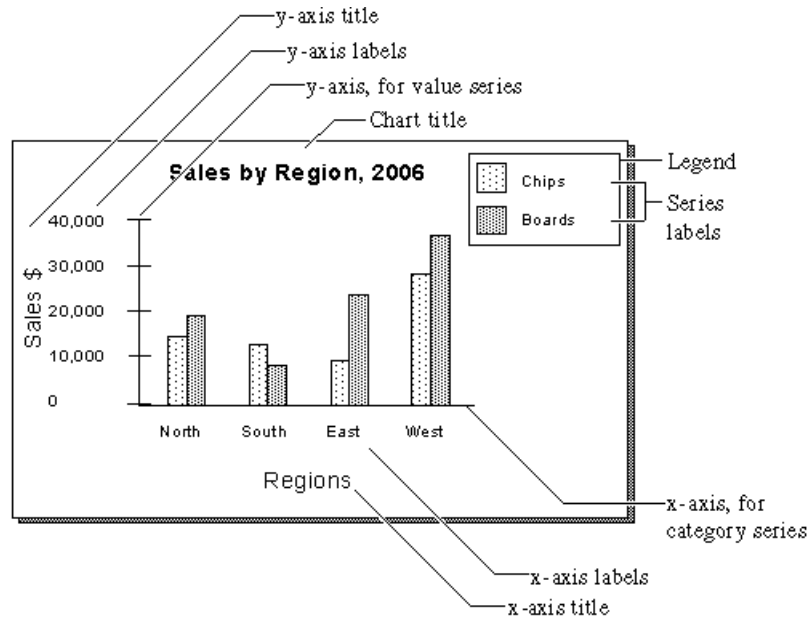
Understanding Charts

A chart is a graphical representation of data or the relationships among data sets. Charts display complex data in an easy-to-assimilate format. In ACS 5.8.1, you cannot customize the charts from Reports web interface.

[Figure 13-9](#) shows the parts of a basic bar chart. A chart displays data as one or more sets of points. The chart organizes data points into sets of values called series. The two types of series are:

- **Category series**—The category series typically determines what text, numbers, or dates you see on the x-axis.
- **Value series**—The value series typically determines the text, numbers, or dates on the y-axis.

In [Figure 13-9](#), the category series contains a set of regions, and the value series contains a set of sales figure values.

Figure 13-9 *Parts of a Basic Bar Chart*

There are a variety of chart types. Some types of data are best depicted with a specific type of chart. Charts can be used as reports in themselves and they can be used together with tabular data report styles.



Troubleshooting ACS with the Monitoring and Report Viewer

This chapter describes the diagnostic and troubleshooting tools that the Monitoring and Report Viewer provides for the Cisco Secure Access Control System.

This chapter contains the following sections:

- [Available Diagnostic and Troubleshooting Tools, page 14-1](#)
- [Performing Connectivity Tests, page 14-3](#)
- [Downloading ACS Support Bundles for Diagnostic Information, page 14-4](#)
- [Working with Expert Troubleshooter, page 14-5](#)

Available Diagnostic and Troubleshooting Tools

The Monitoring and Report Viewer provides the following:

- [Connectivity Tests, page 14-1](#)
- [ACS Support Bundle, page 14-1](#)
- [Expert Troubleshooter, page 14-2](#)

Connectivity Tests

When you have authentication problems, you can perform a connectivity test to check for connectivity issues. You can enter the hostname or the IP address of the network device that you are trying to connect with and execute the following commands from the web interface: **ping**, **tracert**, and **nslookup**.

The Monitoring and Report Viewer displays the output of these commands. See [Performing Connectivity Tests, page 14-3](#) for detailed instructions on how to perform the connectivity tests.

ACS Support Bundle

You can use the ACS support bundle to prepare diagnostic information for TAC to troubleshoot problems with ACS.

Support bundles typically contain the ACS database, log files, core files, and Monitoring and Report Viewer support files. You can exclude certain files from the support bundle, per ACS node. You can download the support bundle to your local computer. The browser (depending on its configuration) displays the progress of the download and prompts you to save the support bundle to an appropriate location.

- If the ACS server is a primary instance, the support bundle includes an export of the ACS configuration.
- If the ACS server is a secondary instance, the ACS database is not included.
- If the ACS server is a log collector, the support bundle includes an export of the monitoring and report configuration and collected AAA audit and diagnostic logs.
- If the ACS server is not the log collector, the monitoring and reporting configuration is not included in the support bundle. See [Downloading ACS Support Bundles for Diagnostic Information](#), page 14-4 for detailed instructions on how to download ACS support bundles.

Expert Troubleshooter

Expert Troubleshooter is an easy-to-use, web-based troubleshooting utility that helps you diagnose and troubleshoot problems in ACS deployments. It reduces the time that you take to diagnose the problem and provides you detailed instructions on how to resolve the problem.

You can use Expert Troubleshooter to diagnose and troubleshoot passed and failed authentications. For example, if a user is unable to gain access to the network, you can use the Expert Troubleshooter to diagnose the cause of this problem.

Expert Troubleshooter provides you the option to run **show** commands on any network device from the ACS web interface. The output of the **show** command is returned to you in precisely the same manner as the output appears on a console.

You can use Expert Troubleshooter to evaluate the configuration of any network device to see if there are any discrepancies that cause the problem. ACS 5.8.1 supports evaluating communication with network devices over IPv6 along with IPv4.

In addition, Expert Troubleshooter provides you four diagnostic tools for troubleshooting Security Group Access device-related problems.

The Expert Troubleshooter identifies the cause of the problem and lists an appropriate course of action that you can take to resolve the problem. See [Working with Expert Troubleshooter](#), page 14-5 for more information on the various tools that Expert Troubleshooter offers.

[Table 14-1](#) describes the diagnostic tools that ACS 5.8.1 offers:

Table 14-1 *Expert Troubleshooter - Diagnostic Tools*

Diagnostic Tool	Description
RADIUS Authentication Troubleshooting	Troubleshoots a RADIUS authentication. See Troubleshooting RADIUS Authentications , page 14-6 for more information.
Execute Network Device Command	Executes any show command on a network device. See Executing the Show Command on a Network Device , page 14-9 for more information.
Evaluate Configuration Validator	Evaluates the configuration of a network device. See Evaluating the Configuration of a Network Device , page 14-10 for more information.

Table 14-1 Expert Troubleshooter - Diagnostic Tools (continued)

Diagnostic Tool	Description
Trust Sec Tools	
Egress (SGACL) Policy	Compares the Egress Policy (SGACL) between a network device and ACS. See Comparing SGACL Policy Between a Network Device and ACS, page 14-11 for more information.
SXP-IP Mappings	Compares SXP mappings between a device and peers. See Comparing the SXP-IP Mappings Between a Device and its Peers, page 14-12 for more information.
IP User SGT	Compares IP-SGTs on a device with ACS authentication-assigned User-IP-SGT records. See Comparing IP-SGT Pairs on a Device with ACS-Assigned SGT Records, page 14-14 for more information.
Device SGT	Compares device SGT with ACS-assigned SGT. See Comparing Device SGT with ACS-Assigned Device SGT, page 14-15 for more information.

Performing Connectivity Tests

You can test your connectivity to a network device with the device's hostname or IP address. For example, you can verify your connection to an identity store by performing a connectivity test. In ACS 5.8.1, you can also test the connectivity of remote machines.

To test connectivity between your ACS and a device's hostname or IP address:

- Step 1** Select **Monitoring and Reports > Troubleshooting > Connectivity Tests**.
The Connectivity Tests page appears.
- Step 2** Click the IPv4 or IPv6 radio button to select the appropriate IP address type.
- Step 3** Modify the fields in the Connectivity Tests page as described in [Table 14-2](#).

Table 14-2 Connectivity Tests

Option	Description
Hostname or IP Address	Enter the hostname or IP address of a connection you want to test. Click Clear to clear the hostname or IP address that you have entered.
ping	Click to see the ping command output, where you can view the packets sent and received, packet loss (if any) and the time for the test to complete.
tracert	Click to see the tracert command output, where you can view the intermediary IP addresses (hops) between your ACS and the tested hostname or IP address, and the time for each hop to complete.
nslookup	Click to see the nslookup command output, where you can see the server and IP address of your tested domain name server hostname or IP address.

- Step 4** Click **ping**, **tracert**, or **nslookup**, depending upon your test.
The output of the **ping**, **tracert**, or **nslookup** command appears.

Related Topics

- [Available Diagnostic and Troubleshooting Tools, page 14-1](#)
- [Connectivity Tests, page 14-1](#)
- [ACS Support Bundle, page 14-1](#)
- [Expert Troubleshooter, page 14-2](#)

Downloading ACS Support Bundles for Diagnostic Information

To create and download an ACS support bundle:

Step 1 Select **Monitoring and Reports > Troubleshooting > ACS Support Bundle**.

The ACS Support Bundle page appears with the fields described in [Table 14-3](#):

Table 14-3 ACS Support Bundle Page

Option	Description
Server	Name of an ACS node instance. Click to display the Download Parameters for the Server page, to create and download an ACS support bundle for the ACS node instance.
IP Address	<i>Display only.</i> Indicates the IP address of an associated ACS node.
Node Designation	<i>Display only.</i> Indicates the primary or secondary instance of an associated ACS node.

Step 2 Choose a server and click **Get Support Bundle**.

The Download Parameters for the Server page appears. You can create and download an ACS support bundle for the associated ACS node instance.

**Note**

ACS 5.8.1 allows you to download the support bundle to an IPv6 URL-specified destination.

Step 3 Select the download options you want to incorporate in your ACS support.tar.gz file.

Downloading a support bundle can be slow if the size of the file is extremely large. For faster downloads, do not include core files and View support files in the support bundle.

The options are:

- **Encrypt Support Bundle**—Check this box to encrypt the support bundle. Specify the decrypting password in **Passphrase** and confirm the password in **Confirm Passphrase**.
- **Include full configuration database**—Check this box to have the whole database included in the support bundle. If this option is not checked, only a subset of the database is included in the support bundle. Click **Include sensitive information** or **Exclude sensitive information** to include or exclude sensitive information in the logs.

Sensitive information consists of passwords in the encrypted format, ACS configuration data, and so on.
- **Include debug logs**—Check this check box to include debug logs, then click **All**, or click **Recent** and enter a value from 1 to 999 in the file(s) field to specify which debug logs to include.

- Include local logs—Check this check box to include local logs, then click **All**, or click **Recent** and enter a value from 1 to 999 in the file(s) field to specify which debug logs to include.
- Include core files—Check this check box to include core files, then click **All** or click **Include files from the last** and enter a value from 1 to 365 in the day(s) field.
- Include monitoring and reporting logs—Check this check box to include monitoring and reporting logs, then click **All** or click **Include files from the last** and enter a value from 1 to 365 in the day(s) field.

Specify which monitoring and reporting logs to include:

- AAA Audit
 - AAA Diagnostics
 - System Diagnostics
 - AAA Accounting
 - Administrative and Operational Audit
- Include system logs—Check the check box to include system logs, then click **All** or **Recent** and enter a value from 1 to 999 in the file(s) field.

You can enter a description in the Description field, if you need.

Step 4 Click:

- **Download** to download the support bundle with the options you specified. The support bundle is created and downloaded.
- **Restore Defaults** to clear the changes you made and return to the default settings.



Note

ACS does not pick up the core files while creating or downloading the support bundle for the associated ACS node instance by default. If you want to include the core files in the support bundle, you can check the **Include core files** check box. You can check the **Encrypt Support Bundle** check box to encrypt the support bundle in ACS. It will ensure that the core files are encrypted and included in the supported bundle.

Related Topics

- [Available Diagnostic and Troubleshooting Tools, page 14-1](#)
- [Connectivity Tests, page 14-1](#)
- [ACS Support Bundle, page 14-1](#)
- [Expert Troubleshooter, page 14-2](#)

Working with Expert Troubleshooter

The following sections describe how to use the Expert Troubleshooter diagnostic tools:

- [Troubleshooting RADIUS Authentications, page 14-6](#)
- [Executing the Show Command on a Network Device, page 14-9](#)
- [Evaluating the Configuration of a Network Device, page 14-10](#)

- [Comparing SGACL Policy Between a Network Device and ACS, page 14-11](#)
- [Comparing the SXP-IP Mappings Between a Device and its Peers, page 14-12](#)
- [Comparing IP-SGT Pairs on a Device with ACS-Assigned SGT Records, page 14-14](#)
- [Comparing Device SGT with ACS-Assigned Device SGT, page 14-15](#)

Related Topics

- [Available Diagnostic and Troubleshooting Tools, page 14-1](#)
- [Connectivity Tests, page 14-1](#)
- [ACS Support Bundle, page 14-1](#)
- [Expert Troubleshooter, page 14-2](#)

Troubleshooting RADIUS Authentications

Use the RADIUS Authentication diagnostic tool to troubleshoot issues with RADIUS authentications. To do this, you must:

-
- Step 1** Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.
The Expert Troubleshooter page appears.
- Step 2** Select RADIUS Authentication Troubleshooting from the list of troubleshooting tools.
The RADIUS Authentication Troubleshooter page appears.
- Step 3** Modify the fields as shown in [Table 14-4](#) to filter the RADIUS authentications that you want to troubleshoot.

Table 14-4 *RADIUS Authentication Troubleshooter Page*

Option	Description
Search and select a RADIUS authentication for troubleshooting	
Username	Enter the username of the user whose authentication you want to troubleshoot, or click Select to choose the username from a list. Click Clear to clear the username.
MAC Address	Enter the MAC address of the device that you want to troubleshoot, or click Select to choose the MAC address from a list. Click Clear to clear the MAC address.
Audit Session ID	Enter the audit session ID that you want to troubleshoot. Click Clear to clear the audit session ID.
NAS IP	Enter the NAS IP address or click Select to choose the NAS IP address from a list. Click Clear to clear the NAS IP address.
NAS Port	Enter the NAS port number or click Select to choose a NAS port number from a list. Click Clear to clear the NAS port number.
Authentication Status	Choose the status of your RADIUS authentication from the Authentication Status drop-down list box. The available options are: <ul style="list-style-type: none"> • Pass or Fail • Pass • Fail

Table 14-4 RADIUS Authentication Troubleshooter Page (continued)

Option	Description
Failure Reason	Enter the failure reason or click Select to choose a failure reason from a list. Click Clear to clear the failure reason.
Time Range	Define a time range from the Time Range drop-down list box. The Monitoring and Report Viewer fetches the RADIUS authentication records that are created during this time range. The available options are: <ul style="list-style-type: none"> • Last hour • Last 12 hours • Today • Yesterday • Last 7 days • Last 30 days • Custom
Start Date-Time	(Only 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	(Only 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 the Monitoring and Report Viewer to fetch at a time from the Fetch Number of Records drop-down list. The available options are 10, 20, 50, 100, 200, and 500.
Active Directory Domain Name	Enter the Active Directory domain name. The AD records are fetched only when the AD details are provided.
Active Directory Domain Admin Name	Enter the Active Directory domain administrator name. The AD records are fetched only when the AD details are provided.
Active Directory Domain Admin Password	Enter the Active Directory domain administrator password. The AD records are fetched only when the AD details are provided.

Step 4 Click **Search** to display the RADIUS authentications that match your search criteria.

The Search Result table is populated with the results of your search. The following fields appear in the table: Time, Status, Username, MAC Address, Audit Session ID, Network Device IP, Failure Reason, and Access Service.

Step 5 Choose the RADIUS authentication record from this table that you want to troubleshoot, and click **Troubleshoot**.

The Expert Troubleshooter begins to troubleshoot your RADIUS authentication. The Monitoring and Report Viewer prompts you for additional input, if required.

For example, if the Expert Troubleshooter must connect to a network device, it prompts you for connection parameters and login credentials.



Note

If the RADIUS authentication was done against AD, then ACS asks for AD credentials before it begins the troubleshooting process. You have to enter the AD credentials each time you access these reports.

Step 6 Click the **User Input Required** button and modify the fields as described in [Table 14-5](#).

Step 7 Click **Submit**.

The Progress Details page appears. This page provides a summary and might prompt you for additional input, if required. If the Monitoring and Report Viewer requires additional input, you must click the **Click User Input Required** button. A dialog box appears.

Step 8 Modify the fields in the dialog box as described in [Table 14-5](#) and click **Submit**.

Table 14-5 *Progress Details Page - User Input Dialog Box*

Option	Description
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 from the Protocol drop-down list. Valid options are: <ul style="list-style-type: none"> Telnet SSHv2 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	Check this check box to use the console server.
Console IP Address	(Only if you check the Use Console Server check box) Enter the console IP address.
Advanced (Use these if you see an “Expect timeout error” or you know that the device has non-standard prompt strings)	
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.

Step 9 Click **Done** to return to the Expert Troubleshooter.

The Progress Details page refreshes periodically to display the tasks that are performed as troubleshooting progresses. After the troubleshooting is complete, the Show Results Summary button appears.

Step 10 Click **Show Results Summary**.

The Results Summary page appears with the information described in [Table 14-6](#).

Table 14-6 Results Summary Page

Option	Description
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.

Step 11 Click **Done** to return to the Expert Troubleshooter.

The Monitoring and Report Viewer provides you the diagnosis, steps to resolve the problem, and troubleshooting summary to help you resolve the problem.

**Note**

You can launch the RADIUS authentication troubleshooter from the RADIUS authentication report pages as well. You must drill down to the details page of a particular RADIUS authentication to launch this diagnostic tool.

Related Topics

- [Available Diagnostic and Troubleshooting Tools, page 14-1](#)
- [Connectivity Tests, page 14-1](#)
- [ACS Support Bundle, page 14-1](#)
- [Expert Troubleshooter, page 14-2](#)

Executing the Show Command on a Network Device

The Execute Network Device Command diagnostic tool allows you to run any **show** command on a network device from the ACS web interface. The result of the **show** command is precisely what you would see on a console and can be used to identify problems in the device configuration. To run a **show** command on any network device:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

Step 2 Select **Execute Network Device Command** from the list of troubleshooting tools.

The Expert Troubleshooter page is refreshed and lists the fields described in [Table 14-7](#).

Table 14-7 Execute Show Command on a Network Device

Option	Description
Enter Information	
Network Device IP	Enter the IPv4 or IPv6 address of the network device on which you want to run the show command.
Command	Enter the show command that you want to run.

- Step 3** Click **Run** to run the **show** command on the specified network device.
The Progress Details page appears. The Monitoring and Report Viewer prompts you for additional input.
- Step 4** Click the **User Input Required** button and modify the fields as described in [Table 14-5](#).
- Step 5** Click **Submit** to run the show command on the network device and view the output.

Related Topics

- [Available Diagnostic and Troubleshooting Tools, page 14-1](#)
- [Connectivity Tests, page 14-1](#)
- [ACS Support Bundle, page 14-1](#)
- [Expert Troubleshooter, page 14-2](#)

Evaluating the Configuration of a Network Device

You can use this diagnostic tool to evaluate the configuration of a network device and identify any missing or incorrect configuration. The Expert Troubleshooter compares the configuration on the device with the standard configuration. To do this:

- Step 1** Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.
- Step 2** Click Evaluate Configuration Validator from the list of troubleshooting tools.
The Expert Troubleshooter page is refreshed and lists the fields described in [Table 14-8](#).

Table 14-8 Evaluate Configuration Validator

Option	Description
Enter Information	
Network Device IP	Enter the IPv4 or IPv6 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	Checked by default.
RADIUS	Checked by default.
Device Discovery	Checked by default.
Logging	Checked by default.

Table 14-8 Evaluate Configuration Validator

Option	Description
Web Authentication	Check this check box if you want to compare the web authentication configuration.
Profiler Configuration	Check this check box if you want to compare the Profiler configuration.
SGA	Check this check box if you want to compare Security Group Access configuration.
802.1X	Check this check box if you want to compare the 802.1X configuration, and choose one of the following options: <ul style="list-style-type: none"> • Open Mode • Low Impact Mode (Open Mode + ACL) • High Security Mode (Closed Mode)

Step 3 Click **Run**.

The Progress Details page appears. The Monitoring and Report Viewer prompts you for additional input.

Step 4 Click the **User Input Required** button and modify the fields as described in [Table 14-5](#).

The Troubleshooting Progress Details page appears. The Expert Troubleshooter retrieves the CLI response from the network device. A new window appears and prompts you to select the interfaces for which you want to analyze the interface configuration.

Step 5 Check the check boxes the interfaces that you want to analyze, and click **Submit** to evaluate the configuration of the interfaces.

The Progress Details page appears with a summary.

Step 6 Click **Show Results Summary** to view the troubleshooting summary.

The Results Summary page appears with the information described in [Table 14-6](#). The missing configurations appear in red.

Related Topics

- [Available Diagnostic and Troubleshooting Tools, page 14-1](#)
- [Connectivity Tests, page 14-1](#)
- [ACS Support Bundle, page 14-1](#)
- [Expert Troubleshooter, page 14-2](#)

Comparing SGACL Policy Between a Network Device and ACS

For Security Group Access-enabled devices, ACS assigns an SGACL for every source SGT-destination SGT pair based on the Egress policy matrix that you configure in ACS. The Egress policy diagnostic tool does the following:

1. Connects to the device whose IP address you provide and obtains the ACLs for each source SGT— destination SGT pair.
2. Checks the Egress policy that is configured in ACS and obtains the ACLs for each source SGT— destination SGT pair.

3. Compares the SGACL policy obtained from the network device with the SGACL policy obtained from ACS.
4. Displays the source SGT —destination SGT pair if there is a mismatch. Also, displays the matching entries as additional information.

To compare the SGACL policy between a network device and ACS:

-
- Step 1** Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.
- Step 2** Select **Egress (SGACL) Policy** from the list of troubleshooting tools.
The Expert Troubleshooter page is refreshed and shows the Network Device IP field.
- Step 3** Enter the IP address of the Security Group Access device whose SGACL policy you want to compare with ACS.
- Step 4** Click **Run** to compare the SGACL policy between ACS and the network device.
The Progress Details page appears. The Monitoring and Report Viewer prompts you for additional input.
- Step 5** Click the **User Input Required** button and modify the fields as described in [Table 14-5](#).
- Step 6** Click **Submit**.
The Progress Details page appears with a brief summary of the results.
- Step 7** Click **Show Results Summary** to view the diagnosis and resolution steps.
The Results Summary page appears with the information described in [Table 14-6](#).
-

Related Topics

- [Available Diagnostic and Troubleshooting Tools, page 14-1](#)
- [Connectivity Tests, page 14-1](#)
- [ACS Support Bundle, page 14-1](#)
- [Expert Troubleshooter, page 14-2](#)

Comparing the SXP-IP Mappings Between a Device and its Peers

Security Group Access devices communicate with their peers and learn their SGT values. The Security Exchange Protocol-IP (SXP)-IP Mappings diagnostic tool connects to the device whose IP address you provide and lists the peer devices' IP addresses and SGT values.

You must select one or more of the device's peers. This tool connects to each of the peers that you select and obtains their SGT values to verify that these values are the same as the values that it learned earlier.

Use this diagnostic tool to compare the SXP-IP mappings between a device and its peers. To do this:

-
- Step 1** Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.
- Step 2** Select **SXP-IP Mappings** from the list of troubleshooting tools.
The Expert Troubleshooter page is refreshed and shows the Network Device IP field.
- Step 3** Enter the IP address of the network device.
- Step 4** Click **SXP-IP Mappings** from the list of troubleshooting tools.
The Expert Troubleshooter page refreshes and shows the following field:

Network Device IP—Enter the IP address of the network device.

Step 5 Click **Run**.

The Progress Details page appears. The Monitoring and Report Viewer prompts you for additional input.

Step 6 Click the **User Input Required** button and modify the fields as described in [Table 14-5](#).

The Troubleshooting Progress Details page appears. The Expert Troubleshooter retrieves SGA SXP connections from the network device and again prompts you to select the peer SXP devices.

Step 7 Click the **User Input Required** button.

A new window appears with the fields as described in [Table 14-9](#).

Table 14-9 Peer SXP Devices

Option	Description
Peer SXP Devices	
Peer IP Address	IP address of the peer SXP device.
VRF	VRF instance of the peer device.
Peer SXP Mode	SXP mode of the peer device; for example, whether it is a speaker or a listener.
Self SXP Mode	SXP mode of the network device; for example, whether it is a speaker or a listener.
Connection State	Status of the connection.
Common Connection Parameters	
User Common Connection Parameters	Check this check box to enable common connection parameters for all the peer SXP devices. 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.
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"> Choose the protocol from the Protocol drop-down list box. Valid options are: <ul style="list-style-type: none"> Telnet SSHv2 <p>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"> Enter the port number. The default port number for Telnet is 23 and SSH is 22.
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.

Step 8 Check the check box of the peer SXP devices for which you want to compare the SXP mappings and enter the Common Connection Parameters as described in [Table 14-9](#).

Step 9 Click **Submit**.

The Progress Details page appears with a brief summary of the results.

Step 10 Click **Show Results Summary** to view the diagnosis and resolution steps.

The Results Summary page appears with the information described in [Table 14-6](#).

Related Topics

- [Available Diagnostic and Troubleshooting Tools, page 14-1](#)
- [Connectivity Tests, page 14-1](#)
- [ACS Support Bundle, page 14-1](#)
- [Expert Troubleshooter, page 14-2](#)

Comparing IP-SGT Pairs on a Device with ACS-Assigned SGT Records

For Security Group Access-enabled devices, ACS assigns each user an SGT value through RADIUS authentication. The IP User SGT diagnostic tool connects to the network device whose IP address you provide and does the following:

1. Obtains a list of all IP-SGT assignments on the network device.
2. Checks the RADIUS authentication and accounting records for each IP-SGT pair to find out the IP-SGT-User value that ACS has assigned to it most recently.
3. Displays the IP-SGT pairs in a tabular format and identifies whether the SGT values most recently assigned by ACS and those on the device are the same or different.

Use this diagnostic tool to compare the IP-SGT values on a device with ACS-assigned SGT. To do this:

Step 1 Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.

Step 2 Click **IP User SGT** from the list of troubleshooting tools.

The Expert Troubleshooter page refreshes and lists the fields described in [Table 14-10](#).

Table 14-10 *IP User SGT*

Option	Description
Enter Information	
Network Device IP	Enter the IPv4 or IPv6 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.

Step 3 Click **Run**.

The Progress Details page appears. The Monitoring and Report Viewer prompts you for additional input.

Step 4 Click the **User Input Required** button and modify the fields as described in [Table 14-5](#).

Step 5 Click **Submit**.

The Progress Details page appears with a brief summary of the results.

Step 6 Click **Show Results Summary** to view the diagnosis and resolution steps.

Related Topics

- [Available Diagnostic and Troubleshooting Tools, page 14-1](#)
- [Connectivity Tests, page 14-1](#)
- [ACS Support Bundle, page 14-1](#)
- [Expert Troubleshooter, page 14-2](#)

Comparing Device SGT with ACS-Assigned Device SGT

For Security Group Access-enabled devices, ACS assigns each network device an SGT value through RADIUS authentication. The Device SGT diagnostic tool connects to the network device whose IP address you provide and does the following:

1. Obtains the network device's SGT value.
2. Checks the RADIUS authentication records to determine the SGT value that ACS had assigned to it most recently.
3. Displays the Device-SGT pairs in a tabular format and identifies whether the SGT values are the same or different.

Use this diagnostic tool to compare the device SGT with ACS-assigned device SGT. To do this:

-
- Step 1** Choose **Monitoring and Reports > Troubleshooting > Expert Troubleshooter**.
The Expert Troubleshooter page appears.
- Step 2** Click **Device SGT** from the list of troubleshooting tools.
The Expert Troubleshooter page is refreshed and lists the fields described in [Table 14-11](#).

Table 14-11 *Device SGT*

Option	Description
Enter Information	
Network Device IPs (comma-separated list)	Enter the network device IPv4 or IPv6 addresses (for the device whose SGT you want to compare with the SGT of an ACS-assigned device), separated by commas.
Common Connection Parameters	
Use Common Connection Parameters	<p>Check this check box to use the following common connection parameters for comparison:</p> <ul style="list-style-type: none"> • Username—Enter the username of the network device. • Password—Enter the password. • Protocol—Choose the protocol from the Protocol drop-down list box. Valid options are: <ul style="list-style-type: none"> – Telnet – SSHv2 <p>Telnet is the default option. If you choose SSHv2, you must ensure that SSH connections are enabled on the network device.</p> • Port—Enter the port number. The default port number for Telnet is 23 and SSH is 22.
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.

Step 3 Click **Run**.

The Progress Details page appears with a summary.

Step 4 Click **Show Results Summary** to view the results of device SGT comparison.

The Results Summary page appears with the diagnosis, resolution, and troubleshooting summary.

Related Topics

- [Available Diagnostic and Troubleshooting Tools, page 14-1](#)
- [Connectivity Tests, page 14-1](#)
- [ACS Support Bundle, page 14-1](#)
- [Expert Troubleshooter, page 14-2](#)



Managing System Operations and Configuration in the Monitoring and Report Viewer

This chapter describes the tasks that you must perform to configure and administer the Monitoring and Report Viewer. The Monitoring Configuration drawer allows you to:

- **Manage data**—The Monitoring and Report Viewer handles large volumes of data from ACS servers. Over a period of time, the performance and efficiency of the Monitoring and Report Viewer depends on how well you manage the data.

To do so efficiently, you must back up the data and transfer it to a remote repository on a periodic basis. You can automate this task by scheduling jobs to run periodically. See [Configuring Data Purging and Incremental Backup, page 15-3](#) for more information on data backup.

- **View log collections**—The Monitoring and Report Viewer collects log and configuration data from ACS servers in your deployment, stores the data in the Monitoring and Report Viewer server, and processes it to generate reports and alarms. You can view the details of the logs collected from any of the servers in your deployment. See [Viewing Log Collections, page 15-8](#) for more information.
- **Recovering Log Messages**—The Monitoring and Report Viewer recovers the logging entries that are missed during the log collection. The log messages are missed when the Monitoring and Report Viewer server is down or the connectivity between the Monitoring and Report Viewer and ACS server is broken.

When connectivity is regained, the Monitoring and Report Viewer discovers the entries that were missed, and notifies the ACS server. When the ACS server receives this notification, it resends the entries to the Monitoring and Report Viewer. See [Recovering Log Messages, page 15-12](#) for more information.

- **View scheduled jobs**—The Monitoring and Report Viewer allows you to schedule tasks that you must perform periodically.

For example, you can schedule an incremental or full backup to be run at regular intervals. You can use the Scheduler to view the details of these tasks. See [Viewing Scheduled Jobs, page 15-12](#) for more information on the Scheduler.

- **View process status**—You can view the status of the various processes that run in the Monitoring and Report Viewer. See [Viewing Process Status, page 15-13](#) for more information on the various processes that run in the Monitoring and Report Viewer.
- **View data upgrade status**—After you upgrade from ACS 5.5 or 5.7 to ACS 5.8.1 through the CLI, you must ensure that the Monitoring and Report Viewer data upgrade is complete. You can view the Monitoring and Report Viewer data upgrade status through the web interface and switch the

Monitoring and Report Viewer database if upgrade is complete. See [Viewing Data Upgrade Status, page 15-14](#) for more information.

- Configure and edit failure reasons—The Monitoring and Report Viewer allows you to configure the description of the failure reason code and provide instructions to resolve the problem. See [Viewing Failure Reasons, page 15-15](#) for more information on how to edit the failure reason description and instructions for resolution.
- Configure e-mail settings—You can configure the e-mail server and administrator e-mail address. See [Specifying E Mail Settings, page 15-16](#) for more information.
- Configure collection filters—The Monitoring and Report Viewer provides you the option to filter data that is not used for monitoring or troubleshooting purposes. The data that is filtered is not stored in the database and hence saves much needed disk space. See [Understanding Collection Filters, page 15-19](#) for more information on how to configure collection filters.
- Configure system alarms—System alarms notify you of critical conditions encountered during the execution of the ACS Monitoring and Reporting viewer. You can configure if and how you would like to receive notification of system alarms. See [Configuring System Alarm Settings, page 15-21](#) for more information.
- Configure Syslog targets—If you have configured the Monitoring and Report Viewer to send system alarm notifications as Syslog messages, then you must configure a Syslog target to receive the notification. See [Configuring Alarm Syslog Targets, page 15-21](#) for more information.
- Export Monitoring and Report Viewer data—You can configure a remote database, which could either be an Oracle SID or Microsoft SQL Server to which you can export the Monitoring and Report Viewer data.

You can create and run custom reporting applications using the data in your remote database. See [Configuring Remote Database Settings, page 15-21](#) for more information on how to configure a remote database with the Monitoring and Report Viewer.

ACS provides you the option to schedule jobs in the Monitoring and Report Viewer. By scheduling jobs, you can automate the monitoring tasks to be run at specified intervals. You can view the status of the scheduled jobs, control events, and intervene whenever necessary. You can schedule the following jobs:

- Data Purge
- Backup
- Event notification (system and threshold alarms)
- Export of Monitoring and Report Viewer data to a remote database

This chapter contains the following sections:

- [Configuring Data Purging and Incremental Backup, page 15-3](#)
- [Restoring Data from a Backup, page 15-7](#)
- [Viewing Log Collections, page 15-8](#)
- [Recovering Log Messages, page 15-12](#)
- [Viewing Scheduled Jobs, page 15-12](#)
- [Viewing Process Status, page 15-13](#)
- [Viewing Data Upgrade Status, page 15-14](#)
- [Viewing Failure Reasons, page 15-15](#)
- [Editing Failure Reasons, page 15-15](#)
- [Specifying E Mail Settings, page 15-16](#)

- [Configuring SNMP Preferences, page 15-19](#)
- [Understanding Collection Filters, page 15-19](#)
- [Configuring System Alarm Settings, page 15-21](#)
- [Configuring Alarm Syslog Targets, page 15-21](#)
- [Configuring Remote Database Settings, page 15-21](#)

Configuring Data Purging and Incremental Backup

The Monitoring and Report Viewer database handles large volumes of data. When the database size becomes too large, it slows down all the processes. You do not need all the data all the time. Therefore, to efficiently manage data and to make good use of the disk space, you must back up your data regularly and purge unwanted data that uses up necessary disk space. Purging data deletes it from the database.

Since the Monitoring and Report Viewer database size is large, the backup process takes a long time to complete. The incremental backup option enables you to take a complete backup of your Monitoring and Report Viewer database once and then to back up data incrementally (that is, only the updates are backed up and stored separately) from the next time onwards.

An incremental backup performs a full database backup the first time it is run, and subsequently only backs up the updates that are made to the database. Incremental backups are therefore much faster and make efficient use of disk space. You can also configure the frequency and time of incremental backups.

With incremental backups, multiple backup files are stored in the repository. However, when you restore data from an incremental backup, ACS restores data from all the backup files starting from the full backup and continuing until the latest incremental backup.



Note

If you disable incremental backup for some reason, ensure that you run a full backup the next time before you can continue with incremental backups again.

You can also configure a full database backup and define its frequency and time.

ACS also allows you to run an immediate backup of the full Monitoring and Report Viewer database. However, you cannot concurrently run an incremental backup, full backup, and data purge. If any of these jobs are running, you must wait for a period of 90 minutes before you can begin the next job.



Note

We recommend that you take a full backup the first time and then incrementally back up your data instead of running full backups every time.



Note

It is highly recommended that you schedule a incremental backup daily and a full backup monthly or weekly. Otherwise the database purge process fails to purge data, which in turn leads to disk space issues. The monthly scheduled backups occur on the last day of the month and the weekly scheduled backups occur on the last day of the week.

**Note**

To ensure that your data is backed up before the purge, configure a data repository via the CLI or the ACS web interface (**System Administration > Operations > Software Repositories**). Refer to the *CLI Reference Guide for Cisco Secure Access Control System 5.8.1* for more information on configuring a repository.

If you enable incremental backup, data is purged daily at 4:00 a.m. at the local time zone where the ACS instance that runs the View process is located.

In ACS 5.8.1, the view database is allocated based on the opt partition size. ACS View database is 42 percent of opt partition size.

The following database limitations apply for purging:

- If the database disk usage is greater than 60 percent of the allocated view database size, an alarm is sent to the dashboard.
- If the database disk usage is greater than 80 percent of the allocated view database size, a backup is run immediately followed by a purge until the database disk usage is below 60 percent of the allocated view database size. If the backup fails, check the database disk usage again. The Monitoring and Report Viewer data is purged from the database. The oldest data is purged first.
 - If the database disk usage is greater than 60 percent of the allocated view database size, a backup is run immediately followed by a purge until the database disk usage is below 60 percent of the allocated view database size.
 - If the backup fails and the database disk usage is greater than 60 percent of the allocated view database size, the Monitoring and Report Viewer decides to wait.

For example:

- If you specify that you want to preserve one month of data, and the database size is greater than 100 percent of the allocated view database size within a month, the purge deletes the data on a weekly basis until the database size reaches 80 percent of the allocated view database size.
- If you specify that you want to preserve more than one month (for example, 5 months of data) but the database size is over 80 percent of the allocated view database size, a purge occurs. If the database size remains over 80 percent of the allocated view database size after the purge, an additional month of data is purged, which results in 4 months of data preserved. Before the purge, the database is backed up.
- If the database size is over 100 percent of the allocated view database size, a purge occurs regardless of whether or not a database backup has occurred. If the database size remains over 80 percent of the allocated view database size, additional purges occur until the database is 80 percent of the allocated view database size.

**Note**

If the Incremental backup is configured as ON with no repository configured, database backup will fail and Incremental backup mode will be changed to OFF.

**Note**

When incremental backup is disabled, data is purged at the end of every month (Local time).

You can use the Data Purging and Incremental Backup page to:

- Configure purge window size
- Purge data from the database

- Assign a data repository backup location to manage backup (of the purge job)
- Configure incremental and full backup schedules
- Configure immediate backup.

The ACS Database needs to be compressed as a part of maintenance operation. You can run the **acsview-db-compress** command from acs-config mode to reduce the physical size of the view database when there is a difference between the physical size and actual size of the view database. ACS 5.8.1 stops only the log collector services during compress operation and will be up and running after the compress operation is completed. You need to enable the log recovery feature to recover the log messages that are received during the database compress operation.

In ACS 5.8.1, database compress operation is automated. You can check the **Enable ACS View Database Compress** check box to compress the ACS View database automatically every day at 5 A.M. The database compress operation is run everyday automatically at 5 A.M whenever there is a need.



Note

You need to enable the log recovery option to recover the log messages that may be received during the database compress operation. If the log recovery feature is not enabled, then ACS sends an alert message to enable the log recovery feature.

The following database limitations apply for ACS database compress:

- An automatic database compress operation is started the forthcoming day at 5 A.M as soon as the database size is greater than 80 percent of allocated view database size.
- ACS displays an alert message when the difference between the physical and actual size of the view database is greater than 7 percent of the allocated view database size and less than 36 percent of the allocated view database size. Also, an automatic database compress operation is triggered when the size of the database exceeds 80 percent of allocated view database size to avoid disk space issues.
- ACS displays an alert message when the difference between the physical and actual size of the view database is greater than 36 percent of the allocated view database size.
 - If the log recovery feature is not enabled and the ACS view database compress option is enabled, an automatic database compress operation is triggered only after enabling the log recovery feature when the size of the database exceeds 80 percent of allocated view database size to avoid disk space issues.
 - If the log recovery feature and the ACS view database compress option are enabled, an automatic database compress operation is started to avoid disk space issues. The log collector services are shut down during this operation and will be up and running after the compress operation is completed. Since you have log recovery feature enabled already, any log messages that are received during the database compress operation are recovered after the log collector services are up and running.
 - If the log recovery feature and the ACS view database compress options are not enabled, ACS does not trigger any database compress operation. But, if the size of the database exceeds 80 percent of the allocated view database, an automatic database compress operation is triggered only after enabling the log recovery feature to avoid disk space issues.
 - If the log recovery feature is enabled, and the ACS view database compress option is not enabled, an automatic database compress operation is started when the size of the database exceeds 80 percent of allocated view database size limit to avoid disk space issues. The log collector services are shut down during this operation and will be up and running after the compress operation is completed. Since you have log recovery feature enabled already, any log messages that are received during the database compress operation are recovered after the log collector services are up and running.

**Note**

It is recommended to perform database compress during the maintenance hours. DB compress may take long time depends on the database size. Database compress should be done after the purge operation gets completed.

From the Monitoring and Report Viewer, select **Monitoring Configuration > System Operations > Data Management > Removal and Backup**.

Table 15-1 *Data Purging and Incremental Backup Page*

Option	Description
Data Purging	
Data Repository	Use the drop-down list box to select the data repository backup location to be used during data purging. See the <i>CLI Reference for ACS 5.8.1</i> to add a data repository.
Maximum Stored Data Period <i>num</i> months.	Use the drop-down list box to indicate the number of months, where <i>num</i> is the number of months of data you want to retain in the Monitoring and Report Viewer database.
Enable ACS View Database Compress	Check the Enable ACS View Database Compress check box to compress the ACS View database automatically every day at 5 A.M.
On-Demand Data Purge	
Purge Now	Click Purge Now to purge the data. This purge overrides the purge limits that are already set. Note It is recommended that you make a full backup before doing an on-demand purge.
View Full Database Backup Now	
Data Repository	Use the drop-down list box to select the data repository backup location to store the full database backup.
Backup Now	Click Backup Now to start a full Monitoring and Report Viewer database backup.
Incremental Backup	
On	Click the On radio button to enable incremental backup. If incremental backup is enabled, the delta is backed up.
Off	Click the Off radio button to disable incremental backup.
Configure Incremental View Database Backup	
Data Repository	Use the drop-down list box to select a data repository for the backup files.
Schedule	Use the drop-down list boxes to select the time of the day when you want the incremental backup to run.
Frequency	Use the drop-down list box to choose the frequency at which you want the incremental backup to run. Valid options are: <ul style="list-style-type: none"> Daily Weekly—Typically occurs at the end of every week. Monthly—Typically occurs at the end of every month.
Configure Full View Database Backup	
Data Repository	Use the drop-down list box to select a data repository to store the backup files.

Table 15-1 Data Purging and Incremental Backup Page (continued)

Option	Description
Schedule	Use the drop-down list boxes to select the time of the day when you want the full View database backup to run.
Frequency	Use the drop-down list box to choose the frequency at which you want the full View database backup to run. Valid options are: <ul style="list-style-type: none"> Daily Weekly—Typically occurs at the end of every week. Monthly—Typically occurs at the end of every month.

Configuring NFS Staging

If the utilization of **/opt** exceeds 30 percent, then you are required to use NFS staging with a remote repository to take successful view database backups and generate support bundles. NFS staging uses a Network File System (NFS) share as a staging area of additional disk space during a backup or support bundle request, because these operations are disk space intensive. You can enable NFS staging through ACS CLI using the **backup-staging-url** command. You must provide full permission to NFS directory when you configure the NFS location using the **backup-staging-url** command in ACS 5.8.1 to perform a successful On Demand Backup. For more information on the **backup-staging-url** command, see the [CLI Reference Guide for Cisco Secure Access Control System 5.8.1](#).



Note

This section is not applicable to ACS backup operation, as it does not suffer from the same disk space limitations as the View backup and support bundle generation.



Note

You cannot back up any data when the staging server is down. When the staging server is down, you cannot perform backup and restore operations using any of the configured repositories as they use the same staging server to create the backup file. You have to bring the staging server up or delete the backup staging URL so that the repositories work properly. The backup.tar.gpg file is created under **/opt** during backup operation when the NFS staging URL is not configured. So, before deleting the backup staging URL, you need to make sure that you have enough space in the **/opt** location. The backup operation will fail if ACS does not have enough space in **/opt** location.

Related Topic

[Restoring Data from a Backup, page 15-7](#)

Restoring Data from a Backup

Use this page to restore data from the View database that was backed up earlier. You can restore data from an incremental or full backup. If you choose to restore incremental backup data, ACS restores the full View data backup and then the rest of the incremental backups one at a time in the correct sequence.

To restore data from a backup:

-
- Step 1** Choose **Monitoring Configuration > System Operations > Data Management > Restore**.

The Incremental Backup Restore page appears, displaying the Available Backups to Restore table. [Table 15-2](#) describes the columns in the table.

Table 15-2 *Incremental Backup Restore Page*

Column	Description
Skip View Database backup before Restore	Check this check box to skip the Monitoring and Report Viewer database backup before restoring data from a backup. This option, when checked, hastens the restore process. We recommend that you uncheck this check box because your current data might be lost if a failure occurs during the restore process.
Name	Name of the backup file. The backup filename includes the time stamp; for example, ACSViewBackup-20090618_003400. For an incremental backup, click the Expand icon to view the associated full and incremental backups.
Date	Date on which the backup is run.
Repository	Name of the repository that contains the backup file.
Type	The type of backup, Incremental or Full.

Step 2 Choose a backup file that you want to restore.



Note

If you choose an incremental backup file to restore, ACS restores all previously associated incremental and full backups. This restore process restores only the Monitoring and Report Viewer data.

Step 3 Click **Restore** to restore the backup file.

Related Topic

[Configuring Data Purging and Incremental Backup, page 15-3](#)

Viewing Log Collections

Use this page to view the recently collected logs from ACS servers.

From the Monitoring and Report Viewer, select **Monitoring Configuration > System Operations > Log Collection**.



Note

You can use the refresh symbol to refresh the contents of the page.

Table 15-3 Log Collection Page

Option	Description
ACS Server	Name of the ACS server. Click to open the Log Collection Details page and view recently collected logs.
Last Syslog Message	<p><i>Display only.</i> Indicates the arrival time of the most recent syslog message, in the format <i>Ddd Mmm dd hh:mm:ss timezone yyyy</i>, where:</p> <ul style="list-style-type: none"> Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. Mmm = Jan, Feb, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. dd = A two-digit numeric representation of the day of the month, from 01 to 31. hh = A two-digit numeric representation of the hour of the day, from 00 to 23. mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. ss = A two-digit numeric representation of the second of the minute, from 00 to 59. timezone = The time zone. In a distributed environment, the time zone displayed for all secondary servers corresponds to the time zone of the server in which the view is active. <p>If your primary instance has a time zone of PDT and the secondary instance is in UTC, the secondary instance displays the time zone and timestamp of syslog messages with PDT, which corresponds to the time zone of the primary instance.</p> <ul style="list-style-type: none"> yyyy = A four-digit representation of the year.
Last Error	<i>Display only.</i> Indicates the name of the most recent error message.
Last Error Time	<p><i>Display only.</i> Indicates the arrival time of the most recent error message, in the format <i>Ddd Mmm dd hh:mm:ss timezone yyyy</i>, where:</p> <ul style="list-style-type: none"> Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. Mmm = Jan, Feb, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. dd = A two-digit numeric representation of the day of the month, from 01 to 31. hh = A two-digit numeric representation of the hour of the day, from 00 to 23. mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. ss = A two-digit numeric representation of the second of the minute, from 00 to 59. timezone = The time zone. In a distributed environment, the timezone displayed for all secondary servers corresponds to the timezone of the server in which the view is active. <p>If your primary instance has a timezone of PDT and the secondary instance is in UTC, the secondary instance displays the timezone and timestamp of syslog messages with PDT, which corresponds to the timezone of the primary instance.</p> <ul style="list-style-type: none"> yyyy = A four-digit representation of the year.
Get Details	Click to view recently collected logs for a selected ACS server.

Related Topic

[Log Collection Details Page, page 15-9](#)

Log Collection Details Page

Use this page to view the recently collected log names for an ACS server.

-
- Step 1** From the Monitoring and Report Viewer, select **Monitoring Configuration > System Operations > Log Collection**.
- Step 2** Do one of the following:
- Click the name of an ACS server.
 - Select the radio button of the ACS server name that you want to use to view recently collected logs, and click **Get Details**.



Note You can use the refresh symbol to refresh the contents of the page.

Table 15-4 Log Collection Details Page

Option	Description
Log Name	Name of the log file.
Last Syslog Message	<p><i>Display only.</i> Indicates the arrival time of the most recent syslog message, in the format <i>Ddd Mmm dd hh:mm:ss timezone yyyy</i>, where:</p> <ul style="list-style-type: none"> Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. Mmm = Jan, Feb, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. dd = A two-digit numeric representation of the day of the month, from 01 to 31. hh = A two-digit numeric representation of the hour of the day, from 00 to 23. mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. ss = A two-digit numeric representation of the second of the minute, from 00 to 59. timezone = The time zone. In a distributed environment, the timezone displayed for all secondary servers corresponds to the timezone of the server in which the view is active. <p>If your primary instance has a timezone of PDT and the secondary instance is in UTC, the secondary instance displays the timezone and time stamp of syslog messages with PDT, which corresponds to the timezone of the primary instance.</p> <ul style="list-style-type: none"> yyyy = A four-digit representation of the year.
Last Error	<i>Display only.</i> Indicates the name of the most recent error message.
Last Error Time	<p><i>Display only.</i> Indicates the arrival time of the most recent error message, in the format <i>Ddd Mmm dd hh:mm:ss timezone yyyy</i>, where:</p> <ul style="list-style-type: none"> Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. Mmm = Jan, Feb, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. dd = A two-digit numeric representation of the day of the month, from 01 to 31. hh = A two-digit numeric representation of the hour of the day, from 00 to 23. mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. ss = A two-digit numeric representation of the second of the minute, from 00 to 59. timezone = The time zone. In a distributed environment, the timezone displayed for all secondary servers corresponds to the timezone of the server in which the view is active. <p>If your primary instance has a timezone of PDT and the secondary instance is in UTC, the secondary instance displays the timezone and time stamp of syslog messages with PDT, which corresponds to the timezone of the primary instance.</p> <ul style="list-style-type: none"> yyyy = A four-digit representation of the year.
Back	Click to return to the Log Collection page.
Refresh	Click to refresh the data in this page.

Related Topic

- [Viewing Log Collections, page 15-8](#)

Recovering Log Messages

ACS server sends syslog messages to the Monitoring and Report Viewer for the activities such as passed authentication, failed attempts, authorization, accounting, and so on.

The syslog messages have a sequence number attached. If the Monitoring and Report Viewer goes down or if it is not able to receive messages from ACS, then the Monitoring and Report Viewer retries those missed logs from ACS, using the logging recovery mechanism.

The Monitoring and Report Viewer processes the syslog messages, and identifies any discrepancies in the sequence. In this way, it finds the messages that have been missed.

The Monitoring and Report Viewer then notifies the ACS server to resend the missing log messages. ACS server processes the messages stored in its local store and resends them to the Monitoring and Report Viewer.



Note

For the Recovering Log Messages feature to work as desired, you must enable the Log to Local Target option for the relevant logging categories in ACS under **System Administration > Configuration > Log Configuration > Logging Categories > Global**.

To enable Recovering Log Messages, from the Monitoring and Report Viewer, select **Monitoring Configuration > System Operations > Log Message Recovery**.

Table 15-5 Log Message Recovery Page

Option	Description
Log Message Recovery Option	
On	Enable the log message recovery feature.
Off	Disable the log message recovery feature.
Configure Log Message Recovery Intervals	
Run Every Minute(s)	Set the duration in minutes, at which the recovery should happen.
Run Every Hour(s)	Set the duration in hours, at which the recovery should happen.
Configure Missing Entry count to be re-sent by Collector	
No.of Missing Entries to be re-sent by Collector during recovery at a time	Maximum number of missing entries that can be sent by the ACS server at a time. The default limit is 1000 and the maximum limit is 9999. If you set value higher than this, ACS performance might go down.



Note

View logging recovery will not retrieve the missed logs when the View Logging Recovery feature is disabled and the view is down.

Viewing Scheduled Jobs

Use this page to view the scheduled jobs.

From the Monitoring and Report Viewer, select **Monitoring Configuration > System Operations > Scheduler**.

Table 15-6 Scheduler Status Page

Option	Description
Name	<i>Display only.</i> Name of the job.
Type	<i>Display only.</i> Type of associated job; for example, Incremental Backup Utility, Session Termination, DB Aggregation Event, Database Purge Utility, and so on. This list includes both system- and user-defined jobs.
Owner	<i>Display only.</i> Owner of the associated job—System.
Last Run Time	<i>Display only.</i> Time of the associated job, in the format <i>Ddd Mmm dd hh:mm:ss timezone yyyy</i> , where: <ul style="list-style-type: none"> Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. Mmm = Jan, Feb, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. dd = A two-digit numeric representation of the day of the month, from 01 to 31. hh = A two-digit numeric representation of the hour of the day, from 00 to 23. mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. ss = A two-digit numeric representation of the second of the minute, from 00 to 59. <i>timezone</i> = The time zone. yyyy = A four-digit representation of the year.
Last Run Result	<i>Display only.</i> The result of the last run of the associated job.
Status	<i>Display only.</i> The status of the associated job.

**Note**

When you change any schedule through the ACS web interface, for the new schedule to take effect, you must manually restart the Job Manager process. For more information on the CLI command to restart processes, see [CLI Reference Guide for Cisco Secure Access Control System 5.8.1](#).

Viewing Process Status

Use this page to view the status of processes running in your ACS environment.

From the Monitoring and Report Viewer, select **Monitoring Configuration > System Operations > Process Status**.

**Note**

You can click the refresh symbol to refresh the contents of the page.

Table 15-7 Process Status Page

Option	Description
Process Name	<i>Display only.</i> Name of the process. Options can be: <ul style="list-style-type: none"> • Database • Management (ACS management subsystem) • Ntpd • Runtime (ACS runtime subsystem) • View-alertmanager • View-collector • View-database • View-jobmanager • View-logprocessor
Status	<i>Display only.</i> Indicates the status of the associated process.
CPU Utilization	<i>Display only.</i> Indicates the CPU utilization of the associated process.
Memory Utilization	<i>Display only.</i> Indicates the memory utilization of the associated process.
Uptime	<i>Display only.</i> Indicates the time that the process was started successfully, in the format <i>Ddd Mmm dd hh:mm:ss timezone yyyy</i> , where: <ul style="list-style-type: none"> • Ddd = Sun, Mon, Tue, Wed, Thu, Fri, Sat. • Mmm = Jan, Feb, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec. • dd = A two-digit numeric representation of the day of the month, from 01 to 31. • hh = A two-digit numeric representation of the hour of the day, from 00 to 23. • mm = A two-digit numeric representation of the minute of the hour, from 00 to 59. • ss = A two-digit numeric representation of the second of the minute, from 00 to 59. • <i>timezone</i> = The time zone. • yyyy = A four-digit representation of the year.

Viewing Data Upgrade Status

After you upgrade to ACS 5.8.1, ensure that the Monitoring and Report Viewer database upgrade is complete.

You can do this through the ACS web interface. Refer to the *Installation Guide for Cisco Secure Access Control System 5.8.1* for more information on the upgrade process.

To view the status of Monitoring and Report Viewer data upgrade:

-
- Step 1** From the Monitoring and Report Viewer, select **Monitoring Configuration > System Operations > Data Upgrade Status**.

The Data Upgrade Status page appears with the following information:

- Status—Indicates whether or not the Monitoring and Report Viewer data upgrade is complete.

**Note**

It is recommended not to upgrade ACS during aggregation time. If you upgrade ACS during the aggregation time, ACS View upgrade will fail.

Viewing Failure Reasons

Use this page to view failure reasons.

From the Monitoring and Report Viewer, select **Monitoring Configuration > System Configuration > Failure Reasons Editor**.

[Table 15-8](#) lists the field in the Failure Reasons page.

Table 15-8 *Failure Reasons Page*

Option	Description
Failure Reasons	Description of the possible failure reasons. Click a failure reason name to open the Failure Reasons Editor page.

Related Topic

- [Editing Failure Reasons, page 15-15](#)

Editing Failure Reasons

Use this page to edit failure reasons and include possible resolution steps to assist administrators when they encounter failures.

Step 1 From the Monitoring and Report Viewer, select **Monitoring Configuration > System Configuration > Failure Reasons Editor**.

Step 2 Click:

- The name of the failure reason you want to edit.
- The radio button associated with the failure reason you want to edit, then click **Edit**.

The Failure Reason Editor Page appears as described in [Table 15-9](#).

Table 15-9 Failure Reasons Editor Page

Option	Description
Failure Reason	Display only. The error code and associated failure reason name.
Description	Enter a free text description of the failure reason to assist administrators; use the text tools as needed.
Resolution Steps	Enter a free text description of possible resolution steps for the failure reason to assist administrators; use the text tools as needed.

Related Topic

[Viewing Failure Reasons, page 15-15](#)

Specifying E Mail Settings

Use this page to specify the email server and administrator email address.

From the Monitoring and Report Viewer, choose **Monitoring Configuration > System Configuration > Email Settings**.

Table 15-10 Email Settings Page

Option	Description
Mail Server	Enter a valid IPv4 or IPv6 email host server.
Mail From	Enter the email address name that users will see when they receive email from the system.

SNMP Traps

SNMP traps helps you to monitor the status of ACS processes. If you do not have access to an ACS server, but want to monitor the ACS processes, then you can request the ACS administrator to configure a MIB browser as an SNMP host in the ACS server. After the MIB browser is configured as an SNMP server in ACS, you can monitor the ACS process status from the MIB browser.

ACS 5.4 sends the following generic system traps if you configure the SNMP host from the ACS CLI:

- Cold start—if the device is reloaded.
- Linkup—when Ethernet interface is up.
- Linkdown—when Ethernet interface is down.
- Authentication failure—if the community strings do not match.

But, ACS 5.7 allows you to send traps for ACS process status to the SNMP manager if you configure an SNMP host from the ACS CLI. ACS uses the cron job to trigger these traps. After you configure the SNMP host in the ACS CLI, a cron job starts running every minute and monitors the ACS processes. The first time after you configure the SNMP host, you can see that separate traps are received in the SNMP server for each process that is running in ACS, irrespective of its status. The administrator can verify that

the configured SNMP server is able to receive the traps that are sent from ACS. After that, the traps are sent from ACS only when there is a change in the ACS process status. You can view the SNMP traps using the traps receiver in a MIB browser.

ACS sends traps using the OID of hrSWRunName that belongs to the HOST-RESOURCES MIB and sets the OID value as < ACS PROCESS NAME > - < PROCESS STATUS >.

For instance, runtime - running.

The cron job retrieves the ACS process status from the monit binary. ACS 5.8.1 supports both SNMPv1 and SNMPv2c.

ACS sends traps for the following status to the configured SNMP server:

- Process Start (monitored state)
- Process Stop (not monitored state)
- Execution Failed
- Does not exists

In the SNMP server, for every object, a unique object ID is generated and a value is assigned to the OID. You can find the object with its OID value in the SNMP server. The OID value for a running trap is “running,” and the OID value for not monitored, does not exist, and execution failed traps is “stopped.”

To stop ACS from sending SNMP traps to the SNMP server, remove the SNMP configuration from the ACS CLI. This operation stops sending SNMP traps and polling from the SNMP manager.

Configuring SNMP Server to Receive Traps from ACS

To configure an SNMP server to receive traps from ACS:

-
- Step 1** Log in to the ACS CLI using the CLI username and password.
- Step 2** Enter **config t** to enter configuration mode.
- Step 3** Enter the command **snmp-server host <host_ipaddress> version <snmpversion> <communitystring>**. For more information on this command, see the [CLI Reference Guide for Cisco Secure Access Control System](#).



Note

You must configure both the host and the community string to send traps from ACS to a configured SNMP host.

The SNMP server is now configured. The configured SNMP host will receive the traps from ACS.

SNMP Traps for Monitoring Disk Utilization

ACS has the following pre-defined partitions:

- /
- /storedconfig
- /var

- /altroot
- /usr
- /opt
- /recovery
- /home
- /storeddata
- /localdisk
- /tmp
- /boot
- /dev/shm

You can also run the **show disks** command from ACS CLI to view the list of partitions available in ACS. A fresh ACS server does not have all the above partitions and a few partitions may not be available.

ACS 5.8.1 allows you to send SNMP traps to an SNMP host if any of the above ACS partitions reaches its configured threshold disk utilization value. ACS introduces a new CLI command **snmp-server trap dskThresholdLimit <value>** to configure the threshold percentage for disk utilization. The threshold value in the above command represents the percentage of the available free space. For example, if you configure the threshold limit as 40, then you will receive a trap as soon as a partition reaches 60% of its disk space. That is, a trap is sent when the configured amount of free space is reached. After you configure this command from ACS CLI, a cron job starts running every minute and monitors the ACS partitions one by one. If any one of the partitions reaches its threshold limit, then ACS sends a trap to the configured SNMP server with the disk path and the threshold limit value. Multiple traps are sent if multiple partitions reach its threshold limit. You can view the SNMP traps using the traps receiver in a MIB browser.

Sample SNMP trap for disk utilization:

```
Source: 10.77.243.144 Timestamp: 48 hours 25 minutes 5 seconds SNMP Version: 1
Enterprise:
.iso.org.dod.internet.private.enterprises.ucdavis.dskTable.dskEntry.dskPath
Specific: 0
Generic: enterpriseSpecific
Variable Bindings:

Name: .iso.org.dod.internet.private.enterprises.ucdavis.dskTable.dskEntry.dskPath
Value: [OctetString] /boot
```

Sample SNMP Trap for the threshold value of particular disk partition:

```
Source: 10.77.243.144 Timestamp: 48 hours 25 minutes 5 seconds SNMP Version: 1
Enterprise:
.iso.org.dod.internet.private.enterprises.ucdavis.dskTable.dskEntry.dskPercent
Specific: 0
Generic: enterpriseSpecific
Variable Bindings:

Name: .iso.org.dod.internet.private.enterprises.ucdavis.dskTable.dskEntry.dskPercent
Value: [Integer] 19
```

ACS sends these traps using the OIDs “dskpath” and “dskpercent” that belongs to the UCD-SNMP MIB. When you remove and add an SNMP manager from ACS CLI, you will not receive the traps immediately. You have to wait for at least two minutes after the removal or addition of SNMP manager to receive traps. You can run the **show running config** command to view the configured disk threshold limit.

Configuring SNMP Server for Monitoring Disk Utilization

Before you Begin:

An SNMP host and the community string must be configured. See [Configuring SNMP Server to Receive Traps from ACS, page 15-17](#). To configure an SNMP server to monitor disk partition utilization:

-
- Step 1** Log in to the ACS CLI using the CLI username and password.
- Step 2** Enter **config t** to enter configuration mode.
- Enter the command **snmp-server trap dskThresholdLimit <value>**.
- For more information on this command, see the [CLI Reference Guide for Cisco Secure Access Control System](#).



Note

You must configure both the host and the community string to send traps from ACS to a configured SNMP host.

The SNMP server is now configured to send SNMP traps for monitoring disk utilization.

Configuring SNMP Preferences

You can configure SNMP preferences to authenticate access to MIB objects. The text string that you enter for SNMP preference functions as an embedded password.

To configure SNMP preferences:

-
- Step 1** From the Monitoring and Report Viewer, choose **Monitoring Configuration > System Configuration > SNMP Settings**.
- The SNMP Preferences page appears.
- Step 2** Enter a password in the SNMP V2 Read Community String field to authenticate MIB objects.
- Step 3** Click **Submit**.
-

Understanding Collection Filters

You can create collection filters that allow you to filter and drop syslog events that are not used for monitoring or troubleshooting purposes. When you configure collection filters, the Monitoring and Report Viewer does not record these events in the database and thus saves much needed disk space.



Note

ACS 5.8.1 supports collecting syslog messages from IPv6 sources.

This section contains the following topics:

- [Creating and Editing Collection Filters, page 15-20](#)
- [Deleting Collection Filters, page 15-20](#)

Creating and Editing Collection Filters

Use this page to create or edit collection filters. To do this:

- Step 1** From the Monitoring and Report Viewer, choose **Monitoring Configuration > System Configuration > Collection Filters**.

The Collection Filters page appears.

- Step 2** In the Filters area, do one of the following:
- Click **Create** to create a collection filter.
 - Check the check box of the syslog attribute that you want to edit, then click **Edit**.
 - Check the check box of the syslog attribute that you want to delete, then click **Delete**.

The Add or Edit Collection Filters page described in [Table 15-11](#) appears.

Table 15-11 Add or Edit Collection Filters Page

Option	Description
Syslog Attribute	<ul style="list-style-type: none"> • In the Add Filter page, choose any one of the following syslog attributes: <ul style="list-style-type: none"> – NAS IP Address—IPv4 and IPv6 addresses are supported. – Access Service – MAC Address – User • In the Edit Filter page, this field is Display only.
Value	Enter the value of the syslog attribute: <ul style="list-style-type: none"> • NAS IP Address—Enter the IP address of the NAS that you want to filter. • Access Service—Enter the name of the access service that you want to filter. • MAC Address—Enter the MAC address of the machine that you want to filter. • User—Enter the username of the user you want to filter.

- Step 3** Click **Submit**.

Related Topics

- [Creating and Editing Collection Filters, page 15-20](#)
- [Deleting Collection Filters, page 15-20](#)

Deleting Collection Filters

To delete a collection filter:

-
- Step 1** Choose **Monitoring Configuration > System Configuration > Collection Filters**.
The Collection Filters page appears.
- Step 2** Check the check box of the collection filter or filters that you want to delete, then click **Delete**.
The following message appears:
`Are you sure you want to delete the selected item(s)?`
- Step 3** Click **Yes**.
The Collection Filters page appears without the deleted collection filter.
-

Configuring System Alarm Settings

See [Configuring System Alarm Settings, page 12-37](#) for a description of how to configure system alarm settings.

Configuring Alarm Syslog Targets

See [Understanding Alarm Syslog Targets, page 12-38](#) for a description of how to configure the syslog targets.

Configuring Remote Database Settings

Use this page to configure a remote database to which you can export the Monitoring and Report Viewer data. ACS exports data to this remote database at specified intervals. You can schedule the export job to be run once every 1, 2, 4, 6, 8, 12, or 24 hours. You can also schedule the export job to run every 20 or 40 minutes. You can create custom reporting applications that interact with this remote database. ACS supports the following databases:

- Oracle SQL Developer 12c
- Microsoft SQL Server 2014



Note

ACS does not support remote database with cluster setup.

To configure a remote database:

-
- Step 1** From the Monitoring and Report Viewer, choose **Monitoring Configuration > System Configuration > Remote Database Settings**.
The Remote Database Settings Page appears as described in [Table 15-12](#).

Table 15-12 Remote Database Settings Page

Option	Description
Publish to Remote Database	Check the check box for ACS to export data to the remote database periodically. By default, ACS exports data to the remote database every 4 hours.
Server	Enter the IP address of the remote database.
Port	Enter the port number of the remote database. The default port for Microsoft database is 1433 and the default port for Oracle database is 1521. To change the port number for Oracle database, see Changing the Port Numbers for Oracle Database, page 15-23 .
Username	Enter the username for remote database access.
Password	Enter the password for remote database access.
Export Every Minutes	Choose a time interval from the drop-down list box for ACS to use to export data. Valid options are 20 and 40 minutes. The default interval is 20 minutes. Note If you choose the time interval as 40 minutes, ACS starts the remote database export operation immediately for the first time and it continues to do the operation every 40 minutes from then.
Export Every Hours	Choose a time interval from the drop-down list box for ACS to use to export data. Valid options are 1, 2, 4, 6, 8, 12, and 24 hours. The default interval is 4 hours.
Database Type	The type of remote database that you want to configure: <ul style="list-style-type: none"> Click Microsoft Database radio button to configure a Microsoft database, and enter the name of the remote database. Click Oracle SID radio button to configure an Oracle database, and enter the Oracle service name for the Oracle database.
Download Remote Database schema files	Click this link to download the remote database schema files. The following two schema files are downloaded: <ul style="list-style-type: none"> acsvview_microsoft_schema.sql acsvview_oracle_schema.sql

Step 2 Click **Submit** to configure the remote database.



Note Special characters are not supported in remote database names.



Note You can view the status of your export job in the Scheduler. See [Viewing Scheduled Jobs, page 15-12](#) for more information.



Note If there are two log collector servers that have been configured to export data to a remote database, only one log collector server can export data to the remote database at a time. If a second log collector is pointed to the same remote database, it can cause issues such as over-writing of existing entries in the tables.

Changing the Port Numbers for Oracle Database

To change the port number for Oracle database, complete the following steps:

-
- Step 1** Log in to Oracle database.
- Step 2** Open the command prompt.
- Step 3** Run the command **cd C:\oracle\app\oracle\product\10.2.0\server\BIN**.
- Step 4** Run the command **LSNRCTL status** to find the status of the listener service.
- Step 5** Run the command **LSNRCTL Stop** to stop the listener service.
- Step 6** Go to *C:\oracle\app\oracle\product\10.2.0\server\NETWORK\ADMIN* folder and edit the oracle database port numbers in listener.ora and tnsnames.ora files. You should update the same port number in ACS web interface.
- Step 7** Run the command **LSNRCTL Start** to start the listener service.
- Step 8** Log in to ACS web interface.
- Step 9** From the Monitoring and Report Viewer, choose **Monitoring Configuration > System Configuration > Remote Database Settings to change the oracle database port number**.
- Step 10** Enter the new oracle database port number.
- ACS displays the following message:
- This will require view database restart. Are you sure you want to do this?
- Step 11** Click **OK**.
- For more information, see [Configuring Remote Database Settings, page 15-21](#).
-



Managing System Administrators

System administrators are responsible for deploying, configuring, maintaining, and monitoring the ACS servers in your network. They can perform various operations in ACS through the ACS administrative interface. When you define an administrator in ACS, you assign a password and a role or set of roles that determine the access privilege, the administrator has for various operations.

When you create an administrator account, you initially assign a password, which the administrator can subsequently change through the ACS web interface. Irrespective of the roles that are assigned, the administrators can change their own passwords.

ACS provides the following configurable options to manage administrator passwords:

- Password Complexity—Required length and character types for passwords.
- Password History—Prevents repeated use of same passwords.
- Password Lifetime—Forces the administrators to change passwords after a specified time period.
- Account Inactivity—Disables the administrator account if it has not been in use for a specified time period.
- Password Failures—Disables the administrator account after a specified number of consecutive failed login attempts.

In addition, ACS provides you configurable options that determine the IP addresses from which administrators can access the ACS administrative web interface and the session duration after which idle sessions are logged out from the system.

You can use the Monitoring and Report Viewer to monitor administrator access to the system. The Administrator Access report is used to monitor the administrators who are currently accessing or attempting to access the system.

You can view the Administrator Entitlement report to view the access privileges that the administrators have, the configuration changes that are done by administrators, and the administrator access details. In addition, you can use the Configuration Change and Operational Audit reports to view details of specific operations that each of the administrators perform.

The System Administrator section of the ACS web interface allows you to:

- Create, edit, duplicate, or delete administrator accounts
- Change the password of other administrators
- View predefined roles
- Associate roles to administrators
- Configure authentication settings that include password complexity, account lifetime, and account inactivity

- Configure administrator session setting
- Configure administrator access setting

The first time you log in to ACS 5.8.1, you are prompted for the predefined administrator username (*ACSAdmin*) and required to change the predefined password name (*default*). After you change the password, you can start configuring the system.

The predefined administrator has super administrator permissions—Create, Read, Update, Delete, and eXecute (CRUDX)—to all ACS resources. When you register a secondary instance to a primary instance, you can use any account created on the primary instance. The credentials that you create on the primary instance apply to the secondary instance.


Note

After installation, the first time you log in to ACS, you must do so through the ACS web interface and install the licenses. You cannot log in to ACS through the CLI immediately after installation.

This section contains the following topics:

- [Understanding Administrator Roles and Accounts, page 16-2](#)
- [Configuring System Administrators and Accounts, page 16-3](#)
- [Understanding Roles, page 16-3](#)
- [Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-8](#)
- [Viewing Predefined Roles, page 16-13](#)
- [Configuring Authentication Settings for Administrators, page 16-14](#)
- [Configuring Session Idle Timeout, page 16-17](#)
- [Configuring Administrator Access Settings, page 16-17](#)
- [Working with Administrative Access Control, page 16-18](#)
- [Authenticating Administrators against RADIUS Identity and RSA SecurID Servers, page 16-23](#)
- [Resetting the Administrator Password, page 16-29](#)
- [Changing the Administrator Password, page 16-30](#)

Understanding Administrator Roles and Accounts

The first time you log in to ACS 5.8.1, you are prompted for the predefined administrator username (*ACSAdmin*) and are required to change the predefined password name (*default*). The *acsadmin* account in Cisco Secure ACS, Release 5.8.1, is similar to any other administrator account with the SuperAdmin role. The default *acsadmin* account can now be disabled or deleted, provided you have another recovery administrator account with the SuperAdmin role. The account disablement criteria, such as password lifetime, account disablement, and exceeding failed authentication attempts, also apply to the default *acsadmin* account.

After you change the password, you can start configuring the system. The predefined administrator has super administrator permissions—Create, Read, Update, Delete, and eXecute (CRUDX)—to all ACS resources.

If you do not need granular access control, the SuperAdmin role is most convenient, and this role assigned to the predefined *ACSAdmin* account.

To create further granularity in your access control, follow these steps:

Step 1 Define Administrators. See [Configuring System Administrators and Accounts, page 16-3](#).

Step 2 Associate roles to administrators. See [on page 3Understanding Roles, page 16-3](#).

When these steps are completed, defined administrators can log in and start working in the system.

Understanding Authentication

An authentication request is the first operation for every management session. If authentication fails, the management session is terminated. But if authentication passes, the management session continues until the administrator logs out or the session times out.

ACS 5.8.1 authenticates every login operation by using user credentials (username and password). Then, by using the administrator and role definitions, ACS fetches the appropriate permissions and answers subsequent authorization requests.

The ACS user interface displays the functions and options for which you have the necessary administrator privileges only.



Note

Allow a few seconds before logging back in so that changes in the system have time to propagate.

Related Topics

- [Understanding Administrator Roles and Accounts, page 16-2](#)
- [Configuring System Administrators and Accounts, page 16-3](#)

Configuring System Administrators and Accounts

This section contains the following topics:

- [Understanding Roles, page 16-3](#)
- [Administrator Accounts and Role Association, page 16-7](#)
- [Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-8](#)
- [Viewing Role Properties, page 16-14](#)

Understanding Roles

Roles consist of typical administrator tasks, each with an associated set of permissions. Each administrator can have more than one predefined role, and a role can apply to multiple administrators. As a result, you can configure multiple tasks for a single administrator and multiple administrators for a single task.

You use the Administrator Accounts page to assign roles. In general, a precise definition of roles is the recommended starting point. Refer to [Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-8](#) for more information.

Assigning Roles

You can assign roles to the internal administrator account. ACS 5.8.1 provides two methods to assign roles to internal administrators:

- **Static Role assignment**—Roles are assigned manually to the internal administrator account.
- **Dynamic Role assignment**—Roles are assigned based on the rules in the AAC authorization policy.

Assigning Static Roles

ACS 5.8.1 allows you to assign the administrator roles statically to an internal administrator account. This is applicable only for the internal administrator accounts. If you choose this static option, then you must select the administrator roles for each internal administrator account manually. When an administrator is trying to access the account, if that administrator is configured in an administrator internal identity store with a static role assignment, only the identity policy is executed for authentication. The authorization policy is skipped. After successful execution of the identity policy, the administrator is assigned with the selected role for the administrator account.

Assigning Dynamic Roles

ACS 5.8.1 allows you to assign the administrator roles statically to an internal administrator account.

If the administrator account is configured in an external or internal identity store and has a dynamic role assignment, ACS evaluates the authorization policy and gets a list of administrator roles and use it dynamically or Deny Access as the result. If the Super Admin assigns a dynamic role for an administrator and does not configure the authorization policy, then authorization of that administrator account uses the default value “deny access”. As a result, the authorization for this administrator account is denied. But, if you assign a static role for an administrator, then the authorization policy does not have any impact on authorizing that administrator.

Based on the selected role, ACS authenticates and manages the administrator access restrictions and authentications. If Deny Access is the result of the evaluation, then ACS denies access to the administrator and logs the reason for failure in the customer logs.



Note

The ACS web interface displays only the functions for which you have privileges. For example, if your role is Network Device Admin, the System Administration drawer does not appear because you do not have permissions for the functions in that drawer.

Permissions

A permission is an access right that applies to a specific administrative task. Permissions consist of:

- **A Resource** – The list of ACS components that an administrator can access, such as network resources, or policy elements.
- **Privileges** – The privileges are Create, Read, Update, Delete, and eXecute (CRUDX). Some privileges cannot apply to a given resource. For example, the user resource cannot be executed.

A resource given to an administrator without any privileges means that the administrator has no access to resources. In addition, the permissions are discrete. If the privileges create, update, and delete apply to a resource, the read privilege is not available.

If no permission is defined for an object, the administrator cannot access this object, not even for reading.



Note

You cannot make permission changes.

Predefined Roles

ACS 5.8.1 introduces two new predefined administrator roles called Provisioning Admin and Operations Admin. You can create new administrator accounts using these two new roles. You cannot use these two administrator roles together or along with any other administrator roles while creating administrator accounts.

Table 16-1 shows the predefined roles included in ACS:

Table 16-1 *Predefined Role Descriptions*

Role	Privileges
ChangeAdminPassword	This role is intended for ACS administrators who manage other administrator accounts. This role entitles the administrator to change the password of other administrators.
ChangeUserPassword	This role is intended for ACS administrators who manage internal user accounts. This role entitles the administrator to change the password of internal users.
NetworkDeviceAdmin	<p>This role is intended for ACS administrators who need to manage the ACS network device repository only, such as adding, updating, or deleting devices. This role has the following permissions:</p> <ul style="list-style-type: none"> • Read and write permissions on network devices • Read and write permissions on NDGs and all object types in the Network Resources drawer
OperationsAdmin	<p>This role is a combination of a few of the existing administrator accounts along with some extra resources and privileges.</p> <p>To view the resources and privileges of OperationsAdmin:</p> <ol style="list-style-type: none"> 1. Choose System Administration > Administrators > Roles from ACS web interface. 2. Click the radio button near OperationsAdmin. 3. Click View. <p>ACS displays the resources and privileges associated with OperationsAdmin.</p> <p>OperationsAdmin can be authenticated against external databases similar to other administrators in ACS.</p> <p>Note You cannot combine OperationsAdmin role with any other administrator role while creating administrator accounts.</p> <p>Note You can assign roles, resources, and privileges to ProvisioningAdmin similar to other administrators. But, you cannot assign the OperationsAdmin as a recovery administrator account.</p>

Table 16-1 Predefined Role Descriptions (continued)

Role	Privileges
PolicyAdmin	<p>This role is intended for the ACS policy administrator responsible for creating and managing ACS access services and access policy rules, and the policy elements referenced by the policy rules. This role has the following permissions:</p> <ul style="list-style-type: none"> • Read and write permissions on all the elements used in policies, such as authorization profile, NDGs, IDGs, conditions, and so on • Read and write permissions on services policy
ProvisioningAdmin	<p>This role is a combination of a few of the existing administrator accounts along with some extra resources and privileges.</p> <p>To view the resources and privileges of ProvisioningAdmin:</p> <ol style="list-style-type: none"> 1. Choose System Administration > Administrators > Roles from ACS web interface. 2. Click the radio button near ProvisioningAdmin. 3. Click View. <p>ACS displays the resources and privileges associated with ProvisioningAdmin.</p> <p>ProvisioningAdmin can be authenticated against external databases similar to other administrators in ACS.</p> <p>Note You cannot combine ProvisioningAdmin role with any other administrator role while creating administrator accounts.</p> <p>Note You can assign roles, resources, and privileges to ProvisioningAdmin similar to other administrators. But, you cannot assign the ProvisioningAdmin as a recovery administrator account.</p>
ReadOnlyAdmin	<p>This role is intended for ACS administrators who need read-only access to all parts of the ACS user interface.</p> <p>This role has read-only access to all resources</p>
ReportAdmin	<p>This role is intended for administrators who need access to the ACS Monitoring and Report Viewer to generate and view reports or monitoring data only.</p> <p>This role has read-only access on logs.</p>
SecurityAdmin	<p>This role is required in order to create, update, or delete ACS administrator accounts, to assign administrative roles, and to change the ACS password policy. This role has the following permissions:</p> <ul style="list-style-type: none"> • Read and write permissions on internal protocol users and administrator password policies • Read and write permissions on administrator account settings • Read and write permissions on administrator access settings
SuperAdmin	<p>The Super Admin role has complete access to every ACS administrative function. If you do not need granular access control, this role is most convenient, and this is the role assigned to the predefined <i>ACSAdmin</i> account.</p> <p>This role has Create, Read, Update, Delete, and eXecute (CRUDX) permissions on all resources.</p>

Table 16-1 Predefined Role Descriptions (continued)

Role	Privileges
SystemAdmin	<p>This role is intended for administrators responsible for ACS system configuration and operations. This role has the following permissions:</p> <ul style="list-style-type: none"> • Read and write permissions on all system administration activities except for account definition • Read and write permissions on ACS instances
UserAdmin	<p>This role is intended for administrators who are responsible for adding, updating, or deleting entries in the internal ACS identity stores, which includes internal users and internal hosts. This role has the following permissions:</p> <ul style="list-style-type: none"> • Read and write permissions on users and hosts • Read permission on IDGs

**Note**

At first login, only the Super Admin is assigned to a specific administrator.

Related Topics

- [Administrator Accounts and Role Association, page 16-7](#)
- [Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-8](#)

Changing Role Associations

By design, all roles in ACS are predefined and cannot be changed. ACS allows you to only change role associations. Owing to the potential ramifications on the system's entire authorization status, the ACS Super Admin and SecurityAdmin roles alone have the privilege to change role associations.

Changes in role associations take effect only after the affected administrators log out and log in again. At the new login, ACS reads and applies the role association changes.

**Note**

You must be careful in assigning the ACS Super Admin and SecurityAdmin roles because of the global ramifications of role association changes.

Administrator Accounts and Role Association

Administrator account definitions consist of a name, status, description, e-mail address, password, and role assignment.

**Note**

It is recommended that you create a unique administrator for each person. In this way, operations are clearly recorded in the audit log.

Administrators are authenticated against the internal and external databases.

You can edit and delete existing accounts. However, the web interface displays an error message if you attempt to delete or disable the last super administrator.

Only appropriate administrators can configure identities and certificates. The identities configured in the System Administration drawer are available in the Users and Identity Stores drawer, but they cannot be modified there.

When you create a new administrator, you have an option to choose the type of identity store for the password type. The new administrator is authenticated based on this password type. The password type can be internal administrator, AD, or LDAP. The default value of all the existing administrators is **AdminsIDStore**. The password type has a new association defined to create an association between the administrator account and the identity store. During the internal administrator authentication, if the administrator is present in the internal database, then the value in the password type field is read and populated in the attribute list. If this attribute value is not equal to **AdminsIDStore**, then the authentication is routed to either LDAP or an AD identity store, based on the value that is configured in the password type field. ACS uses PAP authentication to authenticate administrators against AD and LDAP.

Recovery Administrator Account

ACS 5.8.1 requires the system administrator to keep at least one administrator account as a recovery account. If an account is configured as a recovery account, then ACS bypasses the administrator identity policy and authorization policy to authenticate that particular administrator. This recovery administrator account is authenticated against the administrator internal identity store. If you try to access ACS using the recovery account, you are authenticated against internal administrator users, and roles are assigned statically. You can have more than one recovery account. By default, the Super Admin account is set as a recovery account. When you create a new administrator account, ACS does not set that account as a recovery account, but you need to configure it as a recovery account in account settings. A recovery administrator cannot enable password hashing in ACS.

To configure an administrator account as a recovery account, you need to perform the following actions:

- Assign a static role to the administrator account.
- Assign the Super Admin role to the administrator account.
- Do not use the password type to set an external identity store to the administrator account.
- Do not enable password hash.

Related Topics

- [Understanding Roles, page 16-3](#)
- [Creating, Duplicating, Editing, and Deleting Administrator Accounts, page 16-8](#)

Creating, Duplicating, Editing, and Deleting Administrator Accounts

To create, duplicate, edit, or delete an administrator account:

Step 1 Choose **System Administration > Administrators > Accounts**.

The Administrators page appears with a list of configured administrators as described in [Table 16-2](#):

Table 16-2 *Accounts Page*

Option	Description
Status	Current status of this administrator: <ul style="list-style-type: none"> Enabled—This administrator is active. Disabled—This administrator is not active. You cannot log into ACS with a disabled administrator account.
Name	Name of the administrator.
Role(s)	Roles assigned to the administrator.
Description	Description of this administrator.

- Step 2** Do any of the following:
- Click **Create**.
 - Check the check box the account that you want to duplicate and click **Duplicate**.
 - Click the account that you want to modify; or, check the check box for the Name and click **Edit**.
 - Check the check box the account for which you want to change the password and click **Change Password**. See [Resetting Another Administrator's Password, page 16-30](#) for more information.



Note On the Duplicate page, you must change at least the Admin Name.

- Check one or more check boxes the accounts that you want to delete and click **Delete**.

ACS deletes the selected administrator account only if there is at least one recovery administrator account with SuperAdmin role in the ACS database other than the selected administrator account.



Note Firefox does not display a warning message when you try to delete the last recovery administrator account from ACS web interface if you have enabled “Prevent this page from creating additional dialogs” check box.

- Step 3** Complete the Administrator Accounts Properties page fields as described in [Table 16-3](#):

Table 16-3 *Administrator Accounts Properties Page*

Option	Description
General	
Administrator Name	Configured name of this administrator. If you are duplicating a rule, be sure to enter a unique name.
Status	From the Status drop-down menu, select whether the account is enabled or disabled. This option is disabled if you check the Account never disabled check box.
Description	A description of this administrator.
Email Address	Administrator e-mail address. ACS View sends alerts to this e-mail address. ACS uses this email address to notify the internal administrators about their password expiry <i>n</i> days before their password expires.

Table 16-3 Administrator Accounts Properties Page (continued)

Option	Description
Recovery Account	<p>Check this option to configure an account as a recovery account. ACS bypasses the administrator identity policies and authorization policies to authenticate the administrators when you use this option. See Recovery Administrator Account, page 16-8 for more information.</p> <p>Note ACS does not allow you to enable password hashing for the Recovery Administrator accounts. ACS displays the following message when you set an administrator account as a recovery account:</p> <p>Please note that for a valid recovery account, you must enable the account, disable password hash, set assignment type to static, assign the SuperAdmin role, and set password type to the Internal Administrators Store.</p>
Account never disabled	<p>Check to ensure that your account is never disabled. Your account will not be disabled even when:</p> <ul style="list-style-type: none"> Your password expires Your account becomes inactive You exceed the specified number of login retries
Enable Password Hash	<p>Check this check box to enable password hashing using the PBKDF2 of Cisco SSL hashing algorithm to provide enhanced security to the administrator passwords. By default, this option is disabled. This option is applicable only for internal administrators. When you disable this option in the middle, you have to re-configure your password using the Change Password option immediately after disabling this option. For more information, see Enable and Disable Password Hashing for Internal Administrators, page 16-12.</p> <p>Note ACS runtime process must be up and running properly for this option to work properly</p>
Authentication Information	
Password Type	<p>Displays (only AD and LDAP) configured external identity store names, along with internal administrator, which is the default password type. You can choose any identity store from the list.</p> <p>During administrator authentication, if an external identity store is configured for the administrator, then the internal identity store forwards the authentication request to the configured external identity store.</p> <p>If an external identity store is selected, you cannot configure a password for the administrator. The password edit box is disabled.</p> <p>You cannot use identity sequences as external identity stores for the password type.</p> <p>You can change the password type using the Change Password button, which is located in the System Administration > Administrators > Accounts page.</p>
Password	Authentication password.
Confirm Password	Confirmation of the authentication password.
Change password on next login	<p>Check to prompt the user for a new password at the next login.</p> <p>Note If you enable Change password on next login option for an administrator account, then the administrator cannot add ACS instances to a distributed deployment.</p>
Role Assignment	
Available Roles	List of all configured roles. Select the roles that you want to assign for this administrator and click >. Click >> to assign all the roles for this administrator.
Assigned Roles	Roles that apply to this administrator.

Step 4 Click **Submit**.

The new account is saved. The Administrators page appears, with the new account that you created or duplicated.

**Note**

For the administrator accounts whose password type is set as AD, ACS fails the authentication if the “User must change password at next logon” option is enabled in Active Directory.

**Note**

A SuperAdmin with static role assignment can create, assign, or remove SuperAdmin roles for other administrators whereas a SuperAdmin with dynamic role assignment cannot create, assign, or remove SuperAdmin roles for other administrators.

Related Topics

- [Understanding Roles, page 16-3](#)
- [Administrator Accounts and Role Association, page 16-7](#)
- [Viewing Predefined Roles, page 16-13](#)
- [Configuring Authentication Settings for Administrators, page 16-14](#)
- [Exporting Administrator Accounts, page 16-11](#)

Exporting Administrator Accounts

ACS 5.8.1 allows you to export the administrator accounts to a .csv file using the export option available on the Administrator Accounts page. This option exports all administrator accounts that are created and listed in the administrator accounts page to a .csv file. You can save this file to a local drive for audit purposes. You can also encrypt the exported file using an encryption password option. You need this password to decrypt the exported file. However, you cannot import the exported administrator account details back into ACS. For dynamic administrator accounts, the roles column in the exported file is empty. If you have assigned multiple roles for an administrator, a semicolon is used in between the roles. You can also export the administrator accounts from the ACS CLI, but you cannot export administrator accounts using REST PI.

**Note**

To export the administrator accounts, you must have an administrator account with SuperAdmin, SystemAdmin, or UserAdmin roles.

To export the administrator accounts from the ACS web interface:

Step 1 Choose **System Administration > Administrators > Accounts**.

The Administrators page appears with a list of configured administrators as described in [Table 16-2](#).

Step 2 Click **Export**.

The Export properties dialog box appears.

Step 3 Check the check box the **Password** field, and enter the encryption password if you want to encrypt the exported file.

Step 4 Click Start Export.

The Export Progress dialog box appears and displays the progress of the export operation. This dialog box also displays the export logs that helps the user to identify the errors during export operation.

**Note**

To export the administrator accounts from the ACS CLI, run the **export-data administrator <repository> <export_filename> <result_filename> <encryption_type>** command in ACS configuration mode.

Related Topics

- [Understanding Roles, page 16-3](#)
- [Administrator Accounts and Role Association, page 16-7](#)
- [Viewing Predefined Roles, page 16-13](#)
- [Configuring Authentication Settings for Administrators, page 16-14](#)

Enable and Disable Password Hashing for Internal Administrators

You can enable password hashing to enhance security for internal administrators password. You can enable the Enable Password Hash option from ACS Administrator Account page of ACS web interface.

To enhance security of internal administrators' password, ACS 5.8.1 introduces the new feature "Enable Password Hash". If you enable this option, the administrator password is converted into hashes using the PBKDF2 of Cisco SSL hashing algorithm and is stored in the internal database. This feature is applicable only for password based authentications. ACS runtime process must be up and running properly for this option to work properly.

ACS converts the passwords to hashes and stores the same in the internal database if the Enable Password Hashing option while creating internal administrator accounts. When an administrator tries to access ACS using the login password, ACS converts that password to hashes using the PBKDF2 hashing algorithm and compares this hash entry with the entry that is stored in the internal database. ACS allows the administrator to log in only if the password hash value matches with the database hash value. ACS supports enabling password hash in distributed deployments. You cannot enable password hashing if you are a recovery administrator.

For a distributed deployment, the trust communication between ACS instances must be enabled to add a ACS instance as a secondary instance using the administrator account whose password hashing option is enabled. For information on Trust Communication, see [Trust Communication in a Distributed Deployment, page 17-31](#).

To enable password hashing for internal administrators:

Step 1 Choose System Administration > Administrators > Accounts.

The Internal Administrators page appears with the list of available internal administrators.

Step 2 Perform one of the following:

- Click **Create**.
- Check the check box next to the administrator account for which you want to enable password hashing and click **Edit**.

Step 3 Check the **Enable Password Hash** check box.

Step 4 Click **Submit**.

The Password hashing option is enabled for the selected internal administrator.



Note

ACS displays the following error when you enable password hashing for a recovery administrator account and click submit: For a recovery account password hash must be disabled.

To disable password hashing for internal administrators:

Step 1 Choose **System Administration > Administrators > Accounts**.

The Internal Administrators page appears with the list of available internal administrators.

Step 2 Check the check box next to administrator account for which you want to disable password hash and click **Edit**.

Step 3 Uncheck the **Enable Password Hash** check box.

Step 4 Click **Submit**.

The Password hashing option is disabled for the selected internal administrator.



Note

After disabling the **Enable Password Hash** option, you must change the user password immediately.

Step 5 Check the check box next to the administrator account for which you have disabled the password hash option and click **Change Password**.

Step 6 Enter the new password in the **Password** field.

Step 7 Reenter the new password in the **Confirm Password** field.

Step 8 Click **Submit**.

Related Topics

- [Understanding Roles, page 16-3](#)
- [Administrator Accounts and Role Association, page 16-7](#)
- [Viewing Predefined Roles, page 16-13](#)
- [Configuring Authentication Settings for Administrators, page 16-14](#)

Viewing Predefined Roles

See [Table 16-1](#) for description of the predefined roles included in ACS.

To view predefined roles:

Choose **System Administration > Administrators > Roles**.

The Roles page appears with a list of predefined roles. [Table 16-4](#) describes the Roles page fields.

Table 16-4 *Roles Page*

Field	Description
Name	List of all configured roles. See Predefined Roles, page 16-5 for a list of predefined roles.
Description	Description of each role.

Viewing Role Properties

Use this page to view the properties of each role.

Choose **System Administration > Administrators > Roles**, and click a role or choose the role's radio button and click **View**.

The Roles Properties page appears as described in [Table 16-5](#):

Table 16-5 *Roles Properties Page*

Field	Description
Name	Name of the role. If you are duplicating a role, you must enter a unique name as a minimum configuration; all other fields are optional. Roles cannot be created or edited. See Table 16-4 for a list of predefined roles.
Description	Description of the role. See Predefined Roles, page 16-5 for more information.
Permissions List	
Resource	List of available resources.
Privileges	Privileges that can be assigned to each resource. If a privilege does not apply, the privilege check box is dimmed (not available). Row color is irrelevant to availability of a given privilege and is determined by the explicit text in the Privileges column.

Related Topics

- [Understanding Roles, page 16-3](#)
- [Administrator Accounts and Role Association, page 16-7](#)
- [Configuring Authentication Settings for Administrators, page 16-14](#)

Configuring Authentication Settings for Administrators

Authentication settings are a set of rules that enhance security by forcing administrators to use strong passwords, regularly change their passwords, and so on. Any password policy changes that you make apply to all ACS system administrator accounts.

To configure a password policy:

Step 1 Choose **System Administration > Administrators > Settings > Authentication**.

The Password Policies page appears with the Password Complexity and Advanced tabs.

Step 2 In the **Password Complexity** tab, check each check box that you want to use to configure your administrator password.

Table 16-6 describes the fields in the Password Complexity tab.

Table 16-6 Password Complexity Tab

Option	Description
Applies to all ACS system administrator accounts	
Minimum length	Required minimum length; the valid options are 4 to 127.
Password may not contain the username or its characters in reversed order	Check to specify that the password cannot contain the username or reverse username. For example, if your username is john, your password cannot be john or nhoj.
Password may not contain 'cisco' or its characters in reversed order	Check to specify that the password cannot contain the word <i>cisco</i> or its characters in reverse order, that is, <i>ocsic</i> .
Password may not contain " or its characters in reversed order	Check to specify that the password does not contain the string that you enter or its characters in reverse order. For example, if you specify a string, polly, your password cannot be polly or yllop.
Password may not contain repeated characters four or more times consecutively	Check to specify that the password cannot repeat characters four or more times consecutively. For example, you cannot have the string apppple as your password. The letter p appears four times consecutively.
Password must contain at least one character of each of the selected types	
Lowercase alphabetic characters	Password must contain at least one lowercase alphabetic character.
Upper case alphabetic characters	Password must contain at least one uppercase alphabetic character.
Numeric characters	Password must contain at least one numeric character.
Non alphanumeric characters	Password must contain at least one nonalphanumeric character.

Step 3 In the **Advanced** tab, enter the values for the criteria that you want to configure for your administrator authentication process.

Table 16-7 describes the fields in the Advanced tab.

Table 16-7 Advanced Tab

Options	Description
Password History	
Password must be different from the previous <i>n</i> versions	Specifies the number of previous passwords for this administrator to be compared against. This option prevents the administrators from setting a password that was recently used. Valid options are 1 to 99.
Password Lifetime: Administrators are required to periodically change password	
Require a password change after <i>n</i> days	Specifies that the password must be changed after <i>n</i> days; the valid options are 1 to 365. This option, when set, ensures that you change the password after <i>n</i> days.
Disable administrator account after <i>n</i> days if password is not changed	Specifies that the administrator account must be disabled after <i>n</i> days if the password is not changed; the valid options are 1 to 365. ACS does not allow you to configure this option without configuring the Display reminder after <i>n</i> days option.

Table 16-7 Advanced Tab

Options	Description
Send Email for password expiry before n days	Specifies that an email notification a day must be sent to the internal administrators starting from n th day before their password expires if the password is not changed; the valid options are 1 to 365. The default value is 5 days. This option, when set, ensures that an email notification is sent to the internal administrator accounts n days before their password expires. ACS does not allow you to configure this option without configuring the Disable administrator account after n days if password is not changed.
Display reminder after n days	Displays a reminder after n days to change password; the valid options are 1 to 365. This option, when set, only displays a reminder. It does not prompt you for a new password.
Account Inactivity: Inactive accounts are disabled	
Require a password change after n days of inactivity	Specifies that the password must be changed after n days of inactivity; the valid options are 1 to 365. This option, when set, ensures that you change the password after n days. ACS does not allow you to configure this option without configuring the Display reminder after n days option.
Disable administrator account after n days of inactivity	Specifies that the administrator account must be disabled after n days of inactivity; the valid options are 1 to 365. ACS does not allow you to configure this option without configuring the Display reminder after n days option.
Incorrect Password Attempts	
Disable account after n successive failed attempts	Specifies the maximum number of login retries after which the account is disabled; the valid options are 1 to 10.

**Note**

ACS automatically deactivates or disables your account based on your last login, last password change, or number of login retries. The CLI and PI user accounts are blocked and they receive a notification that they can change the password through ACS web interface. If your account is disabled, contact another administrator to enable your account.

Step 4 Click **Submit**.

The administrator password is configured with the defined criteria. These criteria will apply only for future logins.

Related Topics

- [Understanding Roles, page 16-3](#)
- [Administrator Accounts and Role Association, page 16-7](#)
- [Viewing Predefined Roles, page 16-13](#)

Configuring Session Idle Timeout

A GUI session, by default, is assigned a timeout period of 30 minutes. You can configure a timeout period for anywhere from 5 to 90 minutes. The session timeout option is not applicable for the Active Directory and Distributed System Management pages. The AD page is automatically refreshed to verify the AD connectivity status based on the refresh interval that is defined in the application. The Distributed System Management page is automatically refreshed for the configured interval of time. You can configure the refresh interval from the Distributed System Management page of ACS web interface.

To configure the timeout period:

-
- Step 1** Choose **System Administration > Administrators > Settings > Session**.
 - Step 2** The GUI Session page appears.
 - Step 3** Enter the Session Idle Timeout value in minutes. Valid values are 5 to 90 minutes.
 - Step 4** Click **Submit**.
-

**Note**

The CLI client interface has a default session timeout value of 6 hours. You cannot configure the session timeout period in the CLI client interface.

Configuring Administrator Access Settings

ACS 5.8.1 allows you to restrict administrative access to ACS based on the IP address of the remote client. You can filter IP addresses in any one of the following ways:

- [Allow All IP Addresses to Connect, page 16-17](#)
- [Allow Remote Administration from a Select List of IP Addresses, page 16-17](#)
- [Reject Remote Administration from a Select List of IP Addresses, page 16-18](#)

Allow All IP Addresses to Connect

You can choose the Allow all IP addresses to connect option to allow all connections; this is the default option.

Allow Remote Administration from a Select List of IP Addresses

To allow administrators to access ACS remotely:

-
- Step 1** Choose **System Administration > Administrators > Settings > Access**.
The IP Addresses Filtering page appears.
 - Step 2** Click Allow only listed IP addresses to connect radio button.
The IP Range(s) area appears.
 - Step 3** Click **Create** in the IP Range(s) area.

A new window appears. Enter the IPv4 or IPv6 address of the machine from which you want to allow remote access to ACS. Enter a subnet mask for an entire IP address range. ACS checks if the address that is entered is in a format that is supported by IPv4 or IPv6.

Step 4 Click **OK**.

The IP Range(s) area is populated with the IP addresses. Repeat Step 3 to add other IP addresses or ranges for which you want to provide remote access.

Step 5 Click **Submit**.**Reject Remote Administration from a Select List of IP Addresses**

To reject administrators from accessing ACS remotely:

Step 1 Choose **System Administration > Administrators > Settings > Access**.

The IP Addresses Filtering page appears.

Step 2 Click **Reject connections** from listed IP addresses radio button.

The IP Range(s) area appears.

Step 3 Click **Create** in the IP Range(s) area.

A new window appears.

Step 4 Enter the IP address of the machine that you do not want to access ACS remotely. Enter a subnet mask for an entire IP address range.**Step 5** Click **OK**.

The IP Range(s) area is populated with the IP addresses. Repeat Step 3 to add other IP addresses or ranges that you want to reject.

Step 6 Click **Submit**.**Note**

It is possible to reject connection from all IP addresses. You cannot reset this condition through the ACS web interface. However, you can use the following CLI command:

```
access-setting accept-all
```

For more information on this command, see [CLI Reference Guide for Cisco Secure Access Control System 5.8.1](#) for more information.

Working with Administrative Access Control

ACS 5.8.1 introduces a new service type called the Administrative Access Control (AAC) service. The AAC service handles the authentications and authorization of the ACS administrators.

The enhanced AAC web interface includes:

- Policy-based authentication and authorization
- Authentication against an external database is feasible by:
 - Password type on administrator accounts in the Internal Administrators ID store.
 - Configuring the identity policy (the authentication policy) against an external database.

This AAC service is automatically created at the time of installation. You cannot remove or add a new AAC service. AAC is not available under the service selection policy and is automatically selected upon administrator login.

The AAC service identifies a set of policies for administrator login. The policies that are provided within the AAC service are these:

- The Administrator identity policy determines the identity database that is used to authenticate the administrator and also retrieves attributes for the administrator that may be used in subsequent authorization policy.
- The Administrator authorization policy determines the role of the administrator for the session in ACS. The assigned role determines the permission of the administrator. Each role has a predefined list of permissions, and it can be viewed in the roles page.

The AAC service processes these two policies in a sequence. You need to configure both the Administrator identity policy and the Administrator authorization policy. The default for both the policies are:

Identity policy—The default is Internal Identity Store.

Authorization policy—The default is Deny Access.

The AAC service supports only the PAP authentication type. Only the Super Admin is permitted to configure administrator access control.

While upgrading the ACS application to ACS 5.8.1, AAC undergoes the following changes:

- Single AAC service is automatically created during upgrade.
- The identity policy in AAC service is set to Administrators Internal Identity Store.
- All existing administrators are validated with a static role assignment.
- All administrators with the Super Admin role are automatically set as the recovery account.

After upgrading the ACS application to 5.8.1, if the administrator accounts are not updated, the upgraded administrator accounts are authenticated against the administrator internal identity store and get their roles through static assignment. While restoring the backup when upgrading, ACS 5.8.1 takes care of upgrading the schema files as well as the data.

**Note**

Administrator accounts created in external identity stores cannot access CARS mode of ACS CLI. But, they can access acs-config mode of ACS CLI.

This section contains the following topics:

- [Administrator Identity Policy, page 16-19](#)
- [Administrator Authorization Policy, page 16-26](#)

Administrator Identity Policy

The identity policy in administrative access control defines the identity source that ACS uses for authentication and attribute retrieval. The attributes and groups can be retrieved only from the external database. ACS can use the retrieved attributes only in subsequent authorization policies.

The AAC service supports two types of identity policies. They are:

- Single result selection
- Rule-based result selection

Super Admin can configure and modify this policy. You can configure a simple policy, which applies the same identity source for authentication of all requests, or you can configure a rule-based identity policy.

The supported identity methods for a simple policy are:

- Deny Access—Access to the user is denied and no authentication is performed.
- Identity Store—A single identity store.

You can select any one of the following identity stores:

- Internal Administrator ID store
- Active Directory ID store
- LDAP ID store
- RSA SecurID store
- RADIUS Identity store

In cases where Deny Access is selected as the result, the access of the administrator is denied.

In a rule-based policy, each rule contains one or more conditions and a result, which is the identity source to use for authentication.

The supported conditions are these:

- System username
- System time and date
- Administrator client IP address

An identity policy in the AAC service does not support the identity store sequence as a result. You can create, duplicate, edit, and delete rules within the identity policy, and you can enable and disable them.



Caution

If you switch between the simple policy and the rule-based policy pages, you will lose your previously saved policy configuration.

To configure a simple identity policy, complete the following steps:

Step 1 Select **System Administration > Administrative Access Control > Identity**.

By default, the Simple Identity Policy page appears with the fields as described in [Table 16-8](#).

Table 16-8 *Simple Identity Policy Page*

Option	Description
Policy type	<p>Defines the type of policy to configure:</p> <ul style="list-style-type: none"> • Simple—Specifies the result to apply to all requests. • Rule-based—Configures rules to apply different results, depending on the request. <p>If you switch between policy types, you will lose your previously saved policy configuration.</p>
Identity Source	Identity source to apply to all requests. The default is Deny Access. For password-based authentication, choose a single identity store or an identity store sequence.

Step 2 Select an identity source for authentication; or, choose **Deny Access**.

Step 3 Click **Save Changes** to save the policy.

Viewing Rule-Based Identity Policies

Select **System Administration > Administrative Access Control > Identity**.

By default, the Simple Identity Policy page appears with the fields as described in [Table 16-8](#). If it is configured, the Rule-Based Identity Policy page appears with the fields as described in [Table 16-9](#):

Table 16-9 *Rule-Based Identity Policy Page*



Option	Description
Policy type	<p>Defines the type of policy to configure:</p> <ul style="list-style-type: none"> Simple—Specifies the results to apply to all requests. Rule-based—Configures rules to apply different results depending on the request. <p> Caution If you switch between policy types, you will lose your previously saved policy configuration.</p>
Status	<p>The current status of the rule. The rule statuses are:</p> <ul style="list-style-type: none"> Enabled—The rule is active. Disabled—ACS does not apply the results of the rule. Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The Monitor option is especially useful for watching the results of a new rule.
Name	Rule name.
Conditions	Conditions that determine the scope of the policy. This column displays all current conditions in sub columns.
Results	Identity source that is used for authentication as a result of the evaluation of the rule.
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	<p>ACS applies the Default rule when:</p> <ul style="list-style-type: none"> Enabled rules are not matched. No other rules are defined. <p>Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.</p>

Table 16-9 *Rule-Based Identity Policy Page (continued)*

Option	Description
Customize button	<p>Opens the Customize page in which you choose the types of conditions to use in policy rules. A new Conditions column appears in the Policy page for each condition that you add.</p> <hr/> <p> Caution If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.</p> <hr/>
Hit Count button	<p>Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10.</p>

To configure a rule-based policy, see these topics:

- [Creating Policy Rules, page 10-39](#)
- [Duplicating a Rule, page 10-40](#)
- [Editing Policy Rules, page 10-40](#)
- [Deleting Policy Rules, page 10-41](#)

Configuring Identity Policy Rule Properties

You can create, duplicate, or edit an identity policy rule to determine the identity databases that are used to authenticate the administrator and retrieve attributes for the administrator. The retrieval of attributes is possible only if you use an external database.

To display this page, complete the following steps:

-
- Step 1** Choose **System Administration > Administrative Access Control > Identity**, then do one of the following:
- Click **Create**.
 - Check a rule check box, and click **Duplicate**.
 - Click a rule name or check a rule check box, then click **Edit**.
4. Complete the fields as shown in the Identity Rule Properties page, as described in [Table 16-10](#).

Table 16-10 *Identity Rule Properties Page*

Option	Description
General	
Rule Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.

Table 16-10 (continued) Identity Rule Properties Page (continued)

Option	Description
Rule Status	<p>Rule statuses are:</p> <ul style="list-style-type: none"> • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor only. The Monitor option is especially useful for watching the results of a new rule.
Conditions	
conditions	<p>Conditions that you can configure for the rule. By default the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page.</p> <p>The default value for each condition is <i>ANY</i>. To change the value for a condition, check the condition check box, then specify the value.</p> <p>If you check Compound Condition, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-41.</p>
Results	
Identity Source	Identity source to apply to requests. The default is Administrators Internal Identity store. For password-based authentication, choose a single identity store or an identity store sequence.

Authenticating Administrators against RADIUS Identity and RSA SecurID Servers

ACS 5.8.1 supports authenticating administrators against RADIUS Identity and RSA SecurID servers. This feature is available in both the ACS web interface and the ACS configuration mode of ACS CLI. This feature enhances security for administrator authentications by using an One Time Password (OTP) that the RADIUS Identity or RSA SecurID server generates. ACS has the following two use cases for authenticating administrators against external identity sources:

- Administrator account is in ACS. Password type is set as External Identity source. The password type is set as external identity source under **System Administration > Administrators > Accounts**. Therefore, the authentication password for the administrator account must be retrieved from the specified external identity source.
- Administrator account is in external identity source. Therefore, ACS uses the external identity source to verify both the administrator account and its password to authenticate the administrator against the external identity source.

This section contains the following topics:

- [Authenticating Administrators against RADIUS Identity Server, page 16-24](#)
- [Authenticating Administrators against RSA SecurID Server, page 16-24](#)

Authenticating Administrators against RADIUS Identity Server

To authenticate administrators against RADIUS Identity server:

-
- Step 1** Add the RADIUS Identity server in ACS. See [Creating, Duplicating, and Editing RADIUS Identity Servers, page 8-90](#) for more information.
 - Step 2** Add ACS and administrator account in RADIUS Identity server. Refer to the RADIUS Identity server documentation for information on how to perform these operations.
 - Step 3** Choose **System Administration > Administrative Access Control > Identity** in the ACS web interface.
 - Step 4** Click **Single result selection** radio button.
 - Step 5** Select the RADIUS Identity server as Identity Source and click **Save Changes**.
 - Step 6** Log out from the ACS web interface.
 - Step 7** Launch ACS web interface to authenticate the administrator account against RADIUS Identity server for the first time.
 - Step 8** Enter the username in the **Username** field, password set in the RADIUS Identity server in the **Password** field, and click **Login**.

Based on the RADIUS Identity server configuration, ACS might display different messages to the administrators before authenticating them.

ACS allows the administrator to log in to the web interface using the password set in the RADIUS Identity server.



Note

To authenticate ACS administrators against RADIUS Identity server from ACS CLI, use the same procedure discussed above in **acs-config** mode of ACS CLI.

Related Topics

- [Authenticating Administrators against RSA SecurID Server, page 16-24](#)

Authenticating Administrators against RSA SecurID Server

To authenticate administrators against RSA SecurID server as an external identity source:

Setting RSA SecurID Server as external identity source for ACS administrator authentications

- Step 1** Add the RSA SecurID server in ACS. See [Configuring RSA SecurID Agents, page 8-80](#) for more information.
- Step 2** Add ACS and administrator account in RSA SecurID server. See RSA Authentication Manager Administrator's Guide for more information.
- Step 3** Choose **System Administration > Administrative Access Control > Identity** in ACS web interface.
- Step 4** Click **Single result selection** radio button.
- Step 5** Select the RSA SecurID server as Identity Source and click **Save Changes**.

You have now configured RSA SecurID server as the external identity source for authenticating administrators.

Performing First ACS administrator authentication using RSA SecurID Server

- Step 1** Launch ACS web interface.
- Step 2** Enter the username in the **Username** field.
- Step 3** Generate a **Token code** using RSA SecurID device and enter the token code in the **Password** field of ACS web interface and click **Login**.

Based on the RSA SecurID server configuration, ACS may display the following message with a system generated PIN:

PIN: <XXXXXXX> Please remember your new PIN then press Return to continue.



Note

Copy the PIN displayed in the above message and store it in your system. You have to use this PIN to generate the subsequent token codes for logging in to the ACS web interface.

- Step 4** Click **Login**.
- ACS allows the administrator to log in to the web interface. The first administrator authentication against RSA SecurID server is successful.

When you use RSA SecurID server to authenticate administrator account for the first time:

- If you click **Cancel** when ACS displays the challenge message, you must start the authentication procedure from the beginning.
- If you click **Cancel** after ACS displays a system generated PIN, it means that you have canceled the first authentication and you can use the system generated PIN to perform the subsequent authentications.

When you use RSA SecurID server for subsequent administrator authentications, if you enter the wrong passcode, ACS prompts for the correct password. If you enter the correct password now and click **Login**, ACS prompts for the next token code to ensure security.

Performing Subsequent ACS administrator authentications using RSA SecurID Server.

- Step 1** Launch ACS web interface.
- Step 2** Enter the username in the **Username** field.
- Step 3** Enter the system generated PIN that ACS has displayed in the RSA SecurID device and click the arrow icon.
- RSA SecurID device displays a passcode.
- Step 4** Copy the passcode from RSA SecurID device and enter the same in the password field of ACS web interface and click **Login**.

ACS allows the administrator to log in to the web interface. The subsequent administrator authentication against RSA SecurID server is successful.

You can find the administrator authentication related logs in **Monitoring and Reports > Reports > ACS Reports > ACS Instance > ACS Administrator Logins** page.

**Note**

To authenticate ACS administrators against RSA SecurID server from ACS CLI, use the same procedure discussed above in **acs-config** mode of ACS CLI. When you authenticate administrator against RSA SecurID server from ACS CLI, you can see two log entries for a single CLI authentication. One entry is logged against ACS web interface and another one is logged against CLI. Both the entries list the IP address as loop back address (127.0.0.1). The ACS web interface log entry displays the authentication summary and the detailed steps whereas the CLI entry only lists the authentication summary, but not the detailed steps.

**Note**

You can download the RSA SecurID software token from the following link:
<http://www.emc.com/security/rsa-securid/rsa-securid-software-authenticators/ms-windows.htm>

Related Topics

- [Authenticating Administrators against RADIUS Identity Server, page 16-24](#)

Administrator Authorization Policy

The authorization policy in the Administrative Access Control is used for dynamically assigning roles to administrators upon login. The role of the administrator is set according to the rules that are defined in the policy. According to the rules that are defined in the policy, the condition can include attributes and groups if authenticated with an external database. ACS can use the retrieved attributes in subsequent policies.

The authorization policy-based role assignment is applicable for both internal and external administrator accounts. This is the only method that is available to assign roles to the external administrator accounts.

In the administrator authorization policy, each rule contains one or more conditions that are used for authentication and a result.

The supported conditions are:

- System username
- System time and date
- Administrator client IP address
- AD dictionary or LDAP dictionary (external groups and attributes)

Generally, we have also added the possibility to configure authorization policy based on the attributes returned by the RADIUS Identity server.

The administrator identity policy and the password type feature enable administrators to authenticate the requests in external identity stores like Active Directory or LDAP identity stores and to retrieve the administrator groups and attributes. The administrator authorization policy rules can be configured based on these retrieved groups and attributes.

You can configure the administrator authorization policy results with a set of administrator roles that are to be assigned to the administrators.

The supported authorization policy results are:

- Administrator Role Result—One or more administrator roles
- Deny Access—Failed authorization

You can create, duplicate, edit, and delete rules within the authorization policy, and you can enable and disable rules.

Configuring Administrator Authorization Policies

The administrator authorization policy determines the role for ACS administrators.

See [Configuring General Access Service Properties, page 10-13](#) for a description of the AAC Access Service properties page.

Use this page to do the following:

- View rules.
- Delete rules.
- Open pages that enable you to create, duplicate, edit, and customize rules.


Select **System Administration > Administrative Access Control > Authorization > Standard Policy**.

The Administrator Authorization Policy page appears as described in [Table 16-11](#).

Table 16-11 Administrators Authorization Policy Page

Option	Description
Status	Rule statuses are: <ul style="list-style-type: none"> • Enabled—The rule is active. • Disabled—ACS does not apply the results of the rule. • Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor-only. The monitor option is especially useful for watching the results of a new rule.
Name	Name of the rule.
Conditions	Conditions that define the scope of the rule. To change the types of conditions that the rule uses, click the Customize button. You must have previously defined the conditions that you want to use.
Results	Displays the administrator roles that are applied when the corresponding rule is matched. You can customize rule results; a rule can apply administrator roles. The columns that appear reflect the customization settings.
Hit Count	Number of times that the rule is matched. Click the Hit Count button to refresh and reset this column.
Default Rule	ACS applies the Default rule when: <ul style="list-style-type: none"> • Enabled rules are not matched. • No other rules are defined. Click the link to edit the Default Rule. You can edit only the results of the Default Rule; you cannot delete, disable, or duplicate it.

Table 16-11 Administrators Authorization Policy Page (continued)

Option	Description
Customize button	<p>Opens the Customize page in which you choose the types of conditions and results to use in policy rules. The Conditions and Results columns reflect your customized settings.</p> <div>  <p>Caution If you remove a condition type after defining rules, you will lose any conditions that you configured for that condition type.</p> </div>
Hit Count button	Opens a window that enables you to reset and refresh the Hit Count display in the Policy page. See Displaying Hit Counts, page 10-10 .

Configuring Administrator Authorization Rule Properties

Use this page to create, duplicate, and edit the rules to determine administrator roles in the AAC access service.

Select **System Administration > Administrative Access Control > Authorization > Standard Policy**, and click **Create**, **Edit**, or **Duplicate**.

The Administrator Authorization Rule Properties page appears as described in [Table 16-12](#).

Table 16-12 Administrators Authorization Rule Properties Page

Option	Description
General	
Name	Name of the rule. If you are duplicating a rule, you must enter a unique name as a minimum configuration; all other fields are optional.
Status	<p>Rule statuses are as follows:</p> <ul style="list-style-type: none"> Enabled—The rule is active. Disabled—ACS does not apply the results of the rule. Monitor—The rule is active, but ACS does not apply the results of the rule. Results such as hit count are written to the log, and the log entry includes an identification that the rule is monitor-only. The monitor option is especially useful for viewing watching the results of a new rule.
Conditions	
conditions	<p>These are conditions that you can configure for the rule. By default the compound condition appears. You can change the conditions that appear by using the Customize button in the Policy page.</p> <p>The default value for each condition is ANY. To change the value for a condition, check the condition check box, then specify the value.</p> <p>If you check Compound Condition, an expression builder appears in the conditions frame. For more information, see Configuring Compound Conditions, page 10-41.</p>
Results	
Roles	Roles to apply for the rule.

Administrator Login Process

When an administrator logs in to the ACS web interface, ACS 5.8.1 performs the authentication as given below.

If an administrator account is configured as a recovery account in the administrator internal identity store, then ACS bypasses the identity and authorization policies, authenticates the administrator against the administrator internal identity store, and assigns the role statically. If an administrator account is not a recovery account, then ACS proceeds with policy-based authentication.

As a part of policy-based authentication, ACS fetches the AAC service with identity policy and authorization policy configuration. ACS evaluates the identity policy and gets the identity store as a result. If the identity policy result is the administrator internal identity store, then ACS evaluates the password type and retrieves the identity store as the result.

ACS authenticates the administrator against the selected identity store, and retrieves the user groups and user attributes, if the administrator account is configured in an external identity store.

If the administrator account is configured in the internal identity store, and it has a static role assignment, then ACS extracts the list of administrator roles.

If the administrator account is configured in an external or internal identity store and has a dynamic role assignment, ACS evaluates the authorization policy, gets a list of administrator roles, and uses it dynamically, or gets Deny Access as the result.

Based on the selected role, ACS authenticates and manages the administrator access restrictions and authentications. If Deny Access is the result of the evaluation, then ACS denies access to the administrator and logs the reason for failure in the customer logs.



Note

An administrator with Super Admin role has the rights to change the roles and privileges of other administrators.



Note

If the administrator password on the AD or LDAP server is expired or reset, then ACS denies the administrator access to the web interface.

Resetting the Administrator Password

While configuring administrator access settings, it is possible for all administrator accounts to get locked out, with none of the administrators able to access ACS from any IP address in your enterprise. If this happens, you must reset the administrator password from the ACS Config CLI. You must use the following command to reset all administrator passwords:

access-setting accept-all

For more information on this command, refer to [CLI Reference Guide for Cisco Secure Access Control System 5.8.1](#).



Note

You cannot reset the administrator password through the ACS web interface.

Changing the Administrator Password

ACS 5.8.1 introduces a new role Change Admin Password that entitles an administrator to change another administrator's password. If an administrator's account is disabled, any other administrator who is assigned the Change Admin Password role can reset the disabled account through the ACS web interface. This section contains the following topics:

- [Changing Your Own Administrator Password, page 16-30](#)
- [Resetting Another Administrator's Password, page 16-30](#)

Changing Your Own Administrator Password

**Note**

All administrators can change their own passwords. You do not need any special roles to perform this operation.

To change your password:

Step 1 Choose **My Workspace > My Account**.

The My Account page appears. See [My Account Page, page 5-2](#) for valid values.

Step 2 In the **Password field** section, enter the current administrator password.

Step 3 In the New Password field, enter a new administrator password.

Step 4 In the Confirm Password field, re-enter the new administration password.

Step 5 Click **Submit**.

The administrator password is created.

You can also use the **acs reset-password** command to reset your ACS Administrator account password. For more information on this command, refer to [CLI Reference Guide for Cisco Secure Access Control System 5.8.1](#).

Resetting Another Administrator's Password

An internal web administrator who has the Super Admin role or ChangeAdminPassword role can reset or change the passwords for other administrators. To reset another administrator's password:

Step 1 Choose **System Administration > Administrators > Accounts**.

The Accounts page appears with a list of administrator accounts.

Step 2 Check the check box the administrator account for which you want to change the password and click **Change Password**.

The Authentication Information page appears, listing the date when the administrator's password was last changed.

Step 3 In the Password field, enter a new administrator password.

- Step 4** In the Confirm Password field, re-enter the new administrator password.
- Step 5** Check the **Change password on next login** check box for the other administrator to change password at first login.
- Step 6** Click **Submit**.
- The administrator password is reset.
-

Related Topics

- [Configuring Authentication Settings for Administrators, page 16-14](#)
- [Understanding Roles, page 16-3](#)
- [Administrator Accounts and Role Association, page 16-7](#)
- [Viewing Predefined Roles, page 16-13](#)



Configuring System Operations

You can configure and deploy ACS instances so that one ACS instance becomes the *primary instance* and the other ACS instances can be registered to the primary as *secondary instances*. An ACS instance represents ACS software that runs on a network.

An ACS deployment may consist of a single instance, or multiple instances deployed in a distributed manner, where all instances in a system are managed centrally. All instances in a system will have an identical configuration.

Use the Distributed System Management page (**System Administration > Operations > Distributed System Management**) to manage all the instances in a deployment. You can only manage instances from the primary instance. You can invoke the Deployment Operations page from any instance in the deployment, but it only controls the operations on the local server.



Note

You can register any primary instance or any secondary instance to another primary instance; however, the primary instance you wish to register cannot have any secondary instances registered to it.

The primary instance, created as part of the installation process, centralizes the configuration of the registered secondary instances. Configuration changes made in the primary instance are automatically replicated to the secondary instance. You can force a *full replication* to the secondary instance if configuration changes do not replicate to the secondary instance.

This chapter contains:

- [Understanding Distributed Deployment, page 17-2](#)
- [Scheduled Backups, page 17-6](#)
- [Synchronizing Primary and Secondary Instances After Backup and Restore, page 17-9](#)
- [Editing Instances, page 17-10](#)
- [Activating a Secondary Instance, page 17-15](#)
- [Registering a Secondary Instance to a Primary Instance, page 17-16](#)
- [Deregistering Secondary Instances from the Distributed System Management Page, page 17-19](#)
- [Deregistering a Secondary Instance from the Deployment Operations Page, page 17-19](#)
- [Changing the IP address of a Primary Instance from the Primary Server, page 17-23](#)
- [Failover, page 17-23](#)
- [Promoting a Secondary Instance from the Distributed System Management Page, page 17-20](#)
- [Replicating a Secondary Instance from a Primary Instance, page 17-21](#)

- [Creating, Duplicating, Editing, and Deleting Software Repositories](#), page 17-25
- [Managing Software Repositories from the Web Interface and CLI](#), page 17-26
- [Configuring RSA Public Key for Authentication against SFTP Repositories](#), page 17-27
- [Exporting Policies from ACS Web Interface](#), page 17-30
- [Trust Communication in a Distributed Deployment](#), page 17-31

Understanding Distributed Deployment

You can configure multiple ACS servers in a deployment. Within any deployment, you designate one server as the *primary* server and all the other servers are *secondary* servers.

In general, you make configuration changes on the primary server only, and the changes are propagated to all secondary servers, which can then view the configuration data as read-only data. A small number of configuration changes can be performed on a secondary server, including configuration of the server certificate, and these changes remain local to the server.

There is no communication between the secondary servers. Communication happens only between the primary server and the secondary servers. The secondary servers do not know the status of the other secondaries in their deployment.

ACS allows you to deploy an ACS instance behind a firewall. [Table 17-1](#) lists the ports that must be open on the firewall for you to access ACS through the various management interfaces.

Table 17-1 *Ports to Open in Firewalls*

Process	Port
ACS Web Interface/Web Service	443
Database replication	TCP 2638
RADIUS server	<ul style="list-style-type: none"> • 1812 and 1645 (RADIUS authentication and authorization) • 1813 and 1646 (RADIUS accounting) • 3799 (RADIUS COA and POD listen for proxy purpose) <p>If your RADIUS server uses port 1812, ensure that your PIX firewall software is version 6.0 or later. Then, run the following command to use port 1812:</p> <pre>aaa-server radius-authport 1812</pre>
Replication over the Message Bus	TCP 61616
RMI	TCP 2020 (for RMI registry service)
	TCP 2030 (for incoming calls)
SNMP (for request)	UDP 161
SNMP (for notifications)	UDP 162
SSH	22
TACACS+ server	TCP 49 or the port numbers that are configured on TACACS+ Port to listen (1024 to 65535).

Table 17-1 *Ports to Open in Firewalls*

Process	Port
ACS View Collector	UDP 20514
ACS View net flow syslog processing	UDP 9993

The ports that are displayed as a listening port on 127.0.0.1 are not listed in the above table. These ports are not accessible outside ACS instance.

The Distributed System Management page can be used to monitor the status of the servers in a deployment and perform operations on the servers.

ACS 5.8.1 supports one primary and twenty one secondary ACS instances in a large ACS deployment. You can make one secondary instance as a dedicated hot standby secondary instance which can be promoted as a primary instance when the actual primary instance goes down. The medium ACS deployment consists of one primary and thirteen secondary ACS instances. Similarly, you can make one secondary instance as a dedicated hot standby secondary instance which can be promoted as a primary instance when the actual primary instance goes down. Also, all ACS 5.8.1 deployments supports 150,000 AAA clients, 10,350 network device groups, 400,000 users, and 200,000 hosts. ACS 5.8.1 log collector server can handle 2 million records per day and 750 messages per second for stress that are sent from various ACS nodes in the deployment to the log collector server. For more information on ACS server deployments, see [Installation and Upgrade Guide for Cisco Secure Access Control System 5.8.1](#).

In a distributed deployment, if you want to use an administrator account whose password hashing option is enabled to add an ACS instance as a secondary instance to the deployment, then you must enable trust communication between ACS instances in the deployment. For information on Trust Communication, see [Trust Communication in a Distributed Deployment, page 17-31](#).

**Note**

ACS 5.8.1 does not support the large deployment with more than twenty two ACS instances.

Related Topics

- [Activating Secondary Servers, page 17-3](#)
- [Removing Secondary Servers, page 17-4](#)
- [Promoting a Secondary Server, page 17-4](#)
- [Understanding Local Mode, page 17-4](#)
- [Understanding Full Replication, page 17-5](#)
- [Specifying a Hardware Replacement, page 17-6](#)

Activating Secondary Servers

To add a server to a deployment:

- Step 1** From the secondary server, issue a request to register on the primary server by selecting the Deployment Operations option.
- Step 2** Activate the secondary instance on the primary server.

You must activate the secondary instance on the primary instance in order for the secondary instance to receive configuration information; this provides a mechanism of admission control.

However, there is an option to automatically activate newly added secondary instances, rather than performing a manual activation request.

Related Topics

- [Removing Secondary Servers, page 17-4](#)
- [Promoting a Secondary Server, page 17-4](#)
- [Understanding Local Mode, page 17-4](#)
- [Understanding Full Replication, page 17-5](#)
- [Specifying a Hardware Replacement, page 17-6](#)

Removing Secondary Servers

To permanently remove a secondary server from a deployment, you must first deregister the secondary server and then delete it from the primary. You can make the request to deregister a server from either the secondary server to be deregistered or from the primary server.

Related Topics

- [Activating Secondary Servers, page 17-3](#)
- [Understanding Distributed Deployment, page 17-2](#)

Promoting a Secondary Server

There can be one server only that is functioning as the primary server. However, you can promote a secondary server so that it assumes the primary role for all servers in the deployment. The promotion operation is performed either on the secondary server that is to assume the primary role or on the primary server.



Note

When the primary server is down, do not simultaneously promote two secondary servers.

Related Topics

- [Activating Secondary Servers, page 17-3](#)
- [Removing Secondary Servers, page 17-4](#)
- [Understanding Local Mode, page 17-4](#)
- [Understanding Full Replication, page 17-5](#)

Understanding Local Mode

You can use the local mode option:

- If the primary server is unreachable from a secondary server (for example, there is a network disconnection) and a configuration change must be made to a secondary server, you can specify that the secondary server go into *Local Mode*.
- If you want to perform some configuration changes on a trial basis that would apply to only one server and not impact all the servers in your deployment, you can specify that one of your secondary servers go into *Local Mode*.

In Local Mode, you can make changes to a single ACS instance through the local web interface, and the changes take effect on that instance only. The Configuration Audit Report available in the Monitoring and Report Viewer has an option to report only those configuration changes that were made in the local mode.

You can generate this report to record the changes that you made to the secondary server in Local Mode. For more information on reports and how to generate them from ACS, see [Managing Reports, page 13-1](#).

When the connection to the primary server resumes, you can reconnect the disconnected secondary instance in Local Mode to the primary server. From the secondary instance in Local Mode, you specify the Admin username and password to reconnect to the primary instance. All configuration changes made while the secondary server was in Local Mode are lost.

Related Topics

- [Activating Secondary Servers, page 17-3](#)
- [Understanding Full Replication, page 17-5](#)

Understanding Full Replication

Under normal circumstances, each configuration change is propagated to all secondary instances. Unlike ACS 4.x where full replication was performed, in ACS 5.8.1, only the specific changes are propagated. As configuration changes are performed, the administrator can monitor (on the Distributed System Management page) the status of the replication and the last replication ID to ensure the secondary server is up to date.

If configuration changes are not being replicated as expected, the administrator can request a full replication to the server. When you request full replication, the full set of configuration data is transferred to the secondary server to ensure the configuration data on the secondary server is re-synchronized.



Note

Replication on the Message Bus happens over TCP port 61616. Full replication happens over the Sybase DB TCP port 2638.



Warning

ACS management services are started even when a warning message is displayed as connection failed. The services do not get stuck in the initialization stage.

Related Topics

- [Activating Secondary Servers, page 17-3](#)
- [Promoting a Secondary Server, page 17-4](#)
- [Understanding Local Mode, page 17-4](#)

Specifying a Hardware Replacement

You can perform a hardware replacement to allow new or existing ACS instance hardware to re-register to a primary server and take over an existing configuration already present in the primary server. This is useful when an ACS instance fails and needs physical replacement.

To perform the hardware replacement

-
- | | |
|---------------|--|
| Step 1 | From the web interface of the primary instance, you must mark the server to be replaced as deregistered. |
| Step 2 | From the secondary server, register to the primary server.

In addition to the standard administrator credentials for connecting to the primary server (username/password), you must specify the replacement keyword used to identify the configuration in the primary server. The keyword is the hostname of the instance that is to be replaced. |
| Step 3 | You must activate the secondary server on the primary, either automatically or by issuing a manual request. |
-

Related Topics

- [Viewing and Editing a Primary Instance, page 17-10](#)
- [Viewing and Editing a Secondary Instance, page 17-14](#)
- [Activating a Secondary Instance, page 17-15](#)
- [Registering a Secondary Instance to a Primary Instance, page 17-16](#)
- [Deregistering Secondary Instances from the Distributed System Management Page, page 17-19](#)
- [Promoting a Secondary Instance from the Distributed System Management Page, page 17-20](#)
- [Using the Deployment Operations Page to Create a Local Mode Instance, page 17-24](#)

Scheduled Backups

You can schedule backups to be run at periodic intervals. You can schedule backups from the primary web interface. The Scheduled Backups feature backs up ACS configuration data. You can back up data from an earlier version of ACS and restore it to a later version.

Refer to the *Installation and Setup Guide for Cisco Secure Access Control System 5.8.1* for more information on upgrading ACS to later versions.

ACS Backup Encryption

ACS backup is encrypted using a dynamic encryption password. The user is prompted for an encryption password while performing a backup operation. ACS encrypts only the ACS data using a dynamic encryption key. The CARS and ACS view data are encrypted using a static key. Therefore ACS prompts for an encryption password when you run a backup that contains ACS data. The user is prompted for a decryption password while restoring a backup that contains ACS data.

When you run a full backup in ACS, ACS uses the static key to encrypt the CARS and ACS data and makes a .gpg file; whereas the ACS backup data is saved inside this .gpg file as a separate .gpg file using the dynamic encryption password. When you restore the full backup, ACS prompts for the decryption password to decrypt the ACS backup data. ACS decrypts the CARS data and ACS view data using the static key.

The encryption password should have:

- A minimum of 8 characters
- Not more than 32 characters
- At least one upper case letter.
- At least one lower case letter.

Special characters are allowed except:

- `
- \$
- (
-)

ACS displays the password policy if the entered password does not meet the password requirements.



Note

ACS 5.8.1 does not support scheduled backups through the CLI.

Related Topic

[Creating, Duplicating, and Editing Scheduled Backups, page 17-7](#)

Creating, Duplicating, and Editing Scheduled Backups

You can create a scheduled backup only for the primary instance. To create, duplicate, or edit a scheduled backup:

Step 1 Choose **System Administration > Operations > Scheduled Backups**.

The Scheduled Backups page appears. [Table 17-2](#) describes the fields listed in the Scheduled Backups page.

Table 17-2 *Scheduled Backups Page*

Option	Description
Backup Data	
Filename created by backup includes a time stamp and file type information appended to the prefix entered	
Filename Prefix	Enter a filename prefix to which ACS appends the backup time stamp. For example, if you enter ACSBackup as the filename prefix and backup is run on June 05, 2009 at 20:37 hours, then ACS creates the backup file ACSBackup-090506-2037.tar.gpg. Note In ACS web interface, you cannot configure utf-8 characters for a backup filename and a repository name.
Encryption Password	Enter a password to encrypt the ACS backup files.
Confirm Encryption Password	Re-enter the encryption password.
Repository	Click Select to open the Software Update and Backup Repositories dialog box, from which you can select the appropriate repository in which to store the backup file.

Table 17-2 Scheduled Backups Page (continued)

Option	Description
Schedule Options	
Time of Day	<p>Choose the time of the day at which you want ACS to back up the ACS configuration data. Backups can be scheduled on a daily, weekly, or monthly basis.</p> <ul style="list-style-type: none"> Daily—Choose this option for ACS to back up the ACS configuration data at the specified time every day. Weekly—Choose this option and specify the day of the week on which you want ACS to back up the ACS configuration data every week. Monthly—Choose this option and specify the day of the month on which you want ACS to back up the ACS configuration data every month.

Step 2 Click **Submit** to schedule the backup.

Related Topic

[Backing Up Primary and Secondary Instances, page 17-8](#)

Backing Up Primary and Secondary Instances

ACS allows you to encrypt the backup with a password. The backup file encryption is available only for ACS configuration backup. The password-based encryption is not applicable if you choose to obtain only the ADE-OS configuration data backup from secondary ACS instances.

ACS provides you the option to back up the primary and secondary instances at any time apart from the regular scheduled backups. For a primary instance, you can back up the following:

- ACS configuration data only
- ACS configuration data and ADE-OS configuration data

For secondary instances, ACS only backs up the ADE-OS configuration data. In this case, ACS does not prompt for an encryption password.

To run an immediate backup from Distributed System Management page:

Step 1 Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears.

Step 2 From the Primary Instance table or the Secondary Instances table, select the instance that you want to back up.

You can select only one primary instance, but many secondary instances for a backup.

Step 3 Click **Backup**.

The Distributed System Management - Backup page appears with the fields described in [Table 17-3](#).

Table 17-3 Distributed System Management - Backup Page

Option	Description
Backup Data	
Filename created by backup includes a time stamp and file type information appended to the prefix entered	
Filename Prefix	Enter a filename prefix to which ACS appends the backup time stamp. For example, if you enter ACSBackup as the filename prefix and backup is run on June 05, 2009 at 20:37 hours, then ACS creates the backup file ACSBackup-090506-2037.tar.gpg. Note In ACS web interface, you cannot configure utf-8 characters for a backup filename and a repository name.
Encryption Password	Enter the encryption password to encrypt the ACS backup files.
Confirm Encryption Password	Re-enter the encryption password which must match the encryption password exactly.
Repository	Click Select to open the Software Update and Backup Repositories dialog box, from which you can select the appropriate repository in which to store the backup file.
Backup Options (only applicable for primary instances)	
ACS Configuration Backup	Click this option if you want to back up only the ACS configuration data.
ACS Configuration and ADE-OS Backup	Click this option if you want to back up both the ACS configuration data and the ADE-OS configuration data.

Step 4 Click **Submit** to run the backup immediately.

To run an immediate backup from Deployment Operations page:

- Step 1** Choose **System Administration > Operations > Local Operations > Deployment Operations**.
The Deployment Operations page appears.
- Step 2** Click **Backup**.
The Deployment Operations - Backup page appears with the fields described in [Table 17-3](#).
- Step 3** Modify the fields in [Table 17-3](#) and click **Submit** to run the backup immediately.

Related Topic

[Scheduled Backups, page 17-6](#)

Synchronizing Primary and Secondary Instances After Backup and Restore

When you specify that a system backup is restored on a primary instance, the secondary instance is not updated to the newly restored database that is present on the primary instance.

To make sure the secondary instance is updated, from the secondary instance, you need to request a hardware replacement to rejoin the restored primary instance. To do this:

-
- Step 1** Deregister the secondary instance from the primary instance.
- Step 2** From the web interface of the secondary instance, choose **Systems Administration > Operations > Local Operations > Deployment Operations**, then click **Deregister from Primary**.
- Step 3** Choose **Systems Administration > Operations > Local Operations > Deployment Operations**.
This allows you to perform the hardware replacement of the secondary instance to the primary instance again.
- Step 4** Specify the primary hostname or IP address and the administrator credential.
- Step 5** Select **Hardware Replacement** and specify the hostname of the secondary instance.
- Step 6** Click **Register to Primary**.
-

Editing Instances

When you Choose **System Administration > Operations > Distributed System Management**, you can edit either the primary or secondary instance. You can take a backup of primary and secondary instances. The Distributed System Management page allows you to do the following:

- [Viewing and Editing a Primary Instance, page 17-10](#)
- [Viewing and Editing a Secondary Instance, page 17-14](#)
- [Backing Up Primary and Secondary Instances, page 17-8](#)
- [Synchronizing Primary and Secondary Instances After Backup and Restore, page 17-9](#)

Viewing and Editing a Primary Instance

To edit a primary instance:

-
- Step 1** Choose **System Administration > Operations > Distributed System Management**.
The Distributed System Management page appears with two tables:
- **Primary Instance table**—Shows the primary instance.
The primary instance is created as part of the installation process.
 - **Secondary Instances table**—Shows a listing and the status of the secondary instances. See [Viewing and Editing a Secondary Instance, page 17-14](#) for more information.
- The Distributed System Management Page displays the information described in [Table 17-4](#):

Table 17-4 *Distributed System Management Page*

Option	Description
Primary Instance	
Name	Hostname of the primary instance.

Table 17-4 Distributed System Management Page (continued)

Option	Description
IP Address	IP address of the primary instance.
Online Status	Indicates if the primary instance is online or offline. A check mark indicates that the primary instance is online; x indicates that the primary instance is offline.
Replication ID	The transaction ID that identifies the last configuration change on the primary instance. This value increases by 1 for every configuration change. Valid values are 1 to infinity.
Role	Displays the role of the primary instance. If a primary ACS instance is set as a log collector server, the role is displayed as Primary: Log Collector.
Last Update	Time stamp of the last database configuration change. The time stamp is in the form <i>hh:mm dd:mm:yyyy</i> .
Version	Current version of the ACS software running on the primary ACS instance. Valid values can be the version string or, if a software upgrade is initiated, <i>Upgrade in progress</i> .
Description	Description of the primary instance.
Edit	Select the primary instance and click this button to edit the primary instance.
Backup	Select the primary instance and click this button to back up the primary instance. See Backing Up Primary and Secondary Instances, page 17-8 for more information.
Secondary Instances	
Name	Hostname of the secondary instance.
IP Address	IP address of the secondary instance.
Online Status	Indicates if the secondary instance is online or offline. A check mark indicates that the secondary instance is online; x indicates that the secondary instance is offline.
Replication ID	The transaction ID that identifies the last configuration change which is received on a secondary instance from a primary instance. This value increases by 1 for every configuration change. Valid values are 1 to infinity. This number must be the same as the Replication ID in the Primary Instance for the primary and secondary ACS servers to be in sync.
Role	Displays the role of the secondary instance. If a secondary ACS instance is set as a log collector server, the role is displayed as Secondary: Log Collector.
Replication Status	Replication status values are: <ul style="list-style-type: none"> UPDATED—Replication is complete on the secondary instance. Both Management and Runtime services are current with configuration changes from the primary instance. PENDING—Request for full replication has been initiated or the configuration changes made on the primary have not yet been propagated to the secondary. REPLICATING—Replication from the primary to the secondary is processing. LOCAL MODE—The secondary instance does not receive replication updates from the deployment and maintains its own local configuration. DEREGISTERED—The secondary instance is deregistered from the primary instance and is not part of the deployment. INACTIVE—The secondary instance is inactive. You must select this instance and click Activate to activate this instance. **—The communication between the primary instance and the secondary instance is not available now. You need to log in to the specific ACS instance to view the required information.
Replication Time	Time stamp of the last replication. The time stamp is in the form <i>hh:mm dd:mm:yyyy</i> .

Table 17-4 Distributed System Management Page (continued)

Option	Description
Version	Current version of the ACS software running on the secondary ACS instance. Valid values can be the version string or, if a software upgrade is initiated, <i>Upgrade in progress</i> .
Description	Description of the secondary instance.
Edit	Select the secondary instance that you want to edit and click this button to edit it.
Delete	Select the secondary instance that you want to delete and click this button to delete it.
Activate	If the option to auto-activate the newly registered secondary instance is disabled, the secondary is initially placed in the inactive state. Click Activate to activate these inactive secondary instances.
Deregister ¹	<p>Disconnects the secondary instance from the primary instance. Stops the secondary instance from receiving configuration updates from the primary instance. Deregistration restarts the deregistered node.</p> <p>When full replication is in progress on an instance, do not attempt to deregister that instance. Wait until the full replication is complete and the secondary instance is restarted before you deregister the secondary instance.</p>
Promote	<p>Requests to promote a secondary instance to the primary instance. All updates to the current primary instance are stopped so that all replication updates can complete. The secondary instance gets primary control of the configuration when the replication updates complete.</p> <p>The secondary instance must be active before you can promote it to the primary instance.</p>
Full Replication	<p>Replicates the primary instance's database configuration for the secondary instance. ACS is restarted.</p> <p>When full replication is in progress on an instance, do not attempt to deregister that instance. Wait until the full replication is complete and the secondary instance is restarted before you deregister the secondary instance.</p>
Backup	Select the secondary instance that you want to back up and click this button to take a backup. See Backing Up Primary and Secondary Instances, page 17-8 for more information.
Refresh	Click to refresh the Distributed System Management page manually.
Refresh Interval	<p>Select the time interval in seconds for the Distributed System Management page to be refreshed automatically. The default value is 30 seconds. The available options are No Refresh, 15 seconds, 30 seconds, and 60 seconds.</p> <p>If you select:</p> <ul style="list-style-type: none"> • No Refresh—ACS does not refresh the Distributed System Management page automatically. You must click Refresh to refresh the page manually. • 15 seconds—ACS refreshes the Distributed System Management page for every 15 seconds. • 30 seconds—ACS refreshes the Distributed System Management page every for 30 seconds. • 60 seconds—ACS refreshes the Distributed System Management page every for 60 seconds. <p>The selected interval works only when you are in the Distributed System Management page. If you navigate to any other page, ACS resets the refresh interval to its default value.</p> <p>Note The refresh interval does not work when you delete a deregistered secondary instance or instances from the Distributed System Management page.</p>

1. Deregistration restarts the deregistered node, but does not restart ACS. Registration and Full Replication restart ACS because the database is replaced.

**Note**

ACS displays two asterisks “**” in a column when that particular ACS instance information is unavailable. The two asterisks indicate that the communication is not available and you need to log in to that particular ACS instance to view the required information.

**Note**

You will not have session time-outs if you are on the Distributed System Management Page as the page is refreshed automatically at regular intervals.

- Step 1** From the Primary Instance table, click the primary instance that you want to modify, or check the **Name** check box and click **Edit**.
- Step 2** Complete the fields in the Distributed System Management Properties page as described in [Table 17-5](#):

Table 17-5 *Distributed System Management Properties Page*

Option	Description
Instance Data	
Hostname	Name of the ACS host machine.
Launch Session for Local GUI	Click this button to launch a new instance of the selected ACS machine. You are required to log in to the primary or secondary instance. This option appears only when you view or edit another instance.
Role	Specifies a primary or secondary instance or Local.
IP Address	IP address of the primary or secondary instance.
Port	Port for Management service.
MAC Address	MAC address for the instance.
Description	Description of the primary or secondary instance.
Check Secondary Every (only applies for primary instance)	Rate at which the primary instance sends a heartbeat status request to the secondary instance. The default value is 60 seconds. The minimum value is 30 seconds and the maximum value is 30 minutes.
Statistics Polling Period (only applies for primary instance)	Rate at which the primary instance polls the secondary instance for statistical and logging information. During each polling period, the primary server does not send any query to all the secondary servers, but, all ACS servers send their health information to the log collector server. The minimum value is 60 seconds and the maximum value is 30 minutes. However, you can specify a value of 0 which indicates to turn off polling and logging. As a result, the log collector server does not show any health status. The default value is 60 seconds.
Enable Auto Activation for Newly Registered Instances (only applies for primary instance)	Check this check box to automatically activate the registered secondary instance.
Instance Status	
Status	Indicates if the primary instance or secondary instance is online or offline.
Version	The current version of the ACS software.

Table 17-5 Distributed System Management Properties Page (continued)

Option	Description
Replication Status (only applies for secondary instances)	Replication status values are: <ul style="list-style-type: none"> UPDATED—Replication is complete on ACS instance. Both management and runtime services are current with configuration changes from the primary instance. PENDING—Request for full replication has been initiated. REPLICATING—Replication from the primary to the secondary is processing. DEREGISTERED—Deregistered the secondary instance from the primary. N/A—No replication on primary instance.
Last Update Time (only applies for primary instance)	Time stamp of the last database configuration change. The time stamp is in the form <i>hh:mm dd:mm:yyyy</i> .
Last Replication Time (only applies for secondary instances)	Time stamp of the last replication. The time stamp is in the form <i>hh:mm dd:mm:yyyy</i> .
Last Replication ID (only applies for primary instance)	Transaction ID that identifies the last configuration change on the secondary instances. This value increases by 1 for every configuration change. Valid values are 1 to infinity.
Primary Replication ID (only applies for secondary instances)	Transaction ID that identifies the last configuration change on the primary instance. This value increases by 1 for every configuration change. Valid values are 1 to infinity.

Step 3 Click **Submit**.

The Primary Instance table on the Distributed System Management page appears with the edited primary instance.

Related Topics

- [Replicating a Secondary Instance from a Primary Instance, page 17-21](#)
- [Viewing and Editing a Secondary Instance, page 17-14](#)

Viewing and Editing a Secondary Instance

To edit a secondary instance:

Step 1 Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears with two tables:

- Primary Instance table—Shows the primary instance.
- Secondary Instances table—Shows a listing and the status of the secondary instances registered to the primary instance.

See [Table 17-4](#) to view column definitions.

- Step 2** From the Secondary Instances table, click the secondary instances that you want to modify, or check the check box near the secondary instances and click **Edit**.
- Step 3** Complete the fields in the Distributed System Management Properties page as described in [Table 17-5](#).
- Step 4** Click **Submit**.
- The Secondary Instances table on the Distributed System Management page appears with the edited secondary instance.
-

Related Topics

- [Editing Instances, page 17-10](#)
- [Viewing and Editing a Primary Instance, page 17-10](#)

Deleting a Secondary Instance

To delete a secondary instance:

-
- Step 1** Choose **System Administration > Operations > Distributed System Management**.
- The Secondary Instances table on the Distributed System Management page appears with a list of secondary instances.
- Step 2** Deregister the secondary instance you wish to delete. Refer to [Deregistering Secondary Instances from the Distributed System Management Page, page 17-19](#).
- Step 3** Check one or more check boxes near the secondary instances that you want to delete.
- Step 4** Click **Delete**.
- The following warning message appears:
- Are you sure you want to continue deleting the selected instance(s)?
Please note that auto Refresh will be disabled during this operation.
- Step 5** Click **OK**.
- The Secondary Instances table on the Distributed System Management page appears without the deleted secondary instances.
-

Activating a Secondary Instance

To activate a secondary instance:

-
- Step 1** Choose **System Administration > Operations > Distributed System Management**.
- The Distributed System Management page appears with two tables:
- Primary Instance table—Shows the primary instance.
 - Secondary Instances table—Shows a listing and the status of the secondary instances registered to the primary instance.
- See the [Table 17-4](#) to view column descriptions.

- Step 2** From the Secondary Instances table, check the check box near the secondary instances that you want to activate.
- Step 3** Click **Activate**.
- Step 4** The Secondary Instances table on the Distributed System Management page appears with the activated secondary instance. See the [Table 17-5](#) for valid field options.

Related Topics

- [Viewing and Editing a Secondary Instance, page 17-14](#)
- [Deleting a Secondary Instance, page 17-15](#)
- [Replicating a Secondary Instance from a Primary Instance, page 17-21](#)
- [Registering a Secondary Instance to a Primary Instance, page 17-16](#)
- [Deregistering a Secondary Instance from the Deployment Operations Page, page 17-19](#)
- [Promoting a Secondary Instance from the Distributed System Management Page, page 17-20](#)
- [Using the Deployment Operations Page to Create a Local Mode Instance, page 17-24](#)

Registering a Secondary Instance to a Primary Instance

To register a secondary instance to a primary instance:

- Step 1** Log into the machine that will be used as a secondary Instance for another ACS server.
- Step 2** Choose **System Administration > Operations > Local Operations > Deployment Operations**.
The Deployment Operations page appears, displaying the information described in [Table 17-6](#):

Table 17-6 *System Operations: Deployment Operations Page*

Option	Description
Instance Status	
Current Status	Identifies the instance of the node you log into as primary or secondary, and identifies whether you are running in local mode.
Primary Instance	Hostname of the primary instance.
Primary IP	IP address of the primary instance.
Registration (only active for an instance not running in Local Mode)	
Primary Instance	Hostname of the primary server that you wish to register with the secondary instance.
Admin Username	Username of an administrator account.
Admin Password	Password for the administrator's account.
Hardware Replacement	Check to enable a new or existing ACS instance hardware to re-register to a primary instance and acquire the existing configuration already present in the primary instance. This is useful when an instance fails and needs physical replacement.

Table 17-6 System Operations: Deployment Operations Page (continued)

Option	Description
Recovery Keyword	Name of the instance that is to be replaced. This value is the hostname of the system that is being replaced. After you submit this information, this instance connects to the primary instance. The primary instance finds the associated ACS instance records based on the keyword, and marks each record as registered.
Register to Primary	Connects to the remote primary and registers the secondary instance to the primary instance.
Backup	
Backup	Backs up the current instance.
Local Mode	
Admin Username	Username of an administrator account.
Admin Password	Password for the administrators account.
Reconnect This option appears only on the local mode node and prompts you for credentials.	Click Reconnect to reconnect to the primary instance. Once you reconnect to the primary instance, you lose the configuration changes that you have made to the local secondary instance. If you want to retain the configuration changes that you have made to the local secondary instance, you must: <ol style="list-style-type: none"> 1. Deregister the local secondary instance (this instance would become your new primary) 2. Deregister all the instances from the deployment. 3. Register all the instances to the new primary, whose configuration changes you want to retain.
Request Local Mode This option appears only on a registered secondary page.	Request to place the secondary instance in local mode. This enables administrators to make configuration changes only to this instance. Any changes made to the secondary instance are not automatically updated when you reconnect to the primary instance. You must manually enter your changes for the secondary instance.

Table 17-6 System Operations: Deployment Operations Page (continued)

Option	Description
Deregistration	
Deregister from Primary	<p>Deregisters the secondary from the primary instance. The secondary instance retains the database configuration from when it was deregistered. All nodes are marked as deregistered and inactive, and the secondary instance becomes the primary instance.</p> <p>When full replication is in progress on an instance, do not attempt to deregister that instance. Wait until the full replication is complete and the secondary instance is restarted before you deregister the secondary instance.</p>
Promotion	
Promote to Primary	Request to promote a secondary instance to primary instance. All updates to the current primary instance are stopped so that all replication updates can complete. The secondary instance gets primary control of the configuration when the replication updates complete.
Replication	
Force Full Replication	<p>Replicates the primary instance's database configuration for the secondary instance.</p> <p>When full replication is in progress on an instance, do not attempt to deregister that instance. Wait until the full replication is complete and the secondary instance is restarted before you deregister the secondary instance.</p>

**Note**

To join a secondary instance to a primary instance, the SuperAdmin account must be local to ACS. You cannot create a deployment using the Admin accounts in the external DB such as AD, LDAP or RSA.

Step 3 Specify the appropriate values in the Registration Section.

Step 4 Click **Register to Primary**.

The following warning message is displayed.

This operation will register this ACS Instance as a secondary to the specified Primary Instance. ACS will be restarted. You will be required to login again. Do you wish to continue?

Step 5 Click **OK**.

The Secondary Instance is restarted automatically.

The credentials and the configurations that you create on the primary instance are applied to the secondary instance.

Step 6 Register another ACS machine as secondary to the same deployment after the first secondary instance is up and running, successfully. Follow the same procedure to register all the secondary machines on the deployment.

**Note**

Memory utilization of 90% is considered normal in the secondary instance if the log collector is running and the server is under heavy load. If Memory utilization increases beyond 90% and keeps increasing, it may be abnormal and needs to be analyzed.

Deregistering Secondary Instances from the Distributed System Management Page

To deregister secondary instances from the Distributed System Management page:

-
- Step 1** Choose **System Administration > Operations > Distributed System Management**.
The Distributed System Management page appears.
- Step 2** From the Secondary Instances table, check one of check boxes the secondary instances that you want to deregister.
- Step 3** Click **Deregister**.
The system displays the following warning message:
This operation will deregister this server as a secondary with the primary server. ACS will be restarted. You will be required to login again. Do you wish to continue?
- Step 4** Click **OK**.
- Step 5** Log into the ACS machine.
- Step 6** Choose **System Administration > Operations > Distributed System Management**.
The Distributed System Management page appears with the secondary instance deregistered from the primary instance.
-

Related Topics

- [Viewing and Editing a Secondary Instance, page 17-14](#)
- [Deleting a Secondary Instance, page 17-15](#)
- [Activating a Secondary Instance, page 17-15](#)
- [Deregistering a Secondary Instance from the Deployment Operations Page, page 17-19](#)
- [Promoting a Secondary Instance from the Distributed System Management Page, page 17-20](#)
- [Using the Deployment Operations Page to Create a Local Mode Instance, page 17-24](#)

Deregistering a Secondary Instance from the Deployment Operations Page



Note

In this case, the secondary instance is the local machine you are logged in to.

To deregister a secondary instance from the Deployment Operations page:

-
- Step 1** Choose **System Administration > Operations > Local Operations > Deployment Operations**.
The Deployment Operations page appears with the secondary instance that you are logged in to. See [Table 17-6](#) for valid field options.
- Step 2** Click **Deregister from Primary**.

The system displays the following warning message:

This operation will deregister this server as a secondary with the primary server. ACS will be restarted. You will be required to login again. Do you wish to continue?

Step 3 Click **OK**.

Step 4 Log into the ACS machine.

Step 5 Choose **System Administration > Operations > Local Operations > Deployment Operations**.

The Deployment Operations page appears with the secondary instance you were logged in to deregistered from the primary instance.

Related Topics

- [Viewing and Editing a Secondary Instance, page 17-14](#)
- [Deleting a Secondary Instance, page 17-15](#)
- [Activating a Secondary Instance, page 17-15](#)
- [Deregistering Secondary Instances from the Distributed System Management Page, page 17-19](#)
- [Promoting a Secondary Instance from the Distributed System Management Page, page 17-20](#)
- [Using the Deployment Operations Page to Create a Local Mode Instance, page 17-24](#)

Promoting a Secondary Instance from the Distributed System Management Page

To promote a secondary instance to a primary instance from the Distributed System Management page:

Step 1 Choose **System Administration > Operations > Distributed System Management**.

The Distributed System Management page appears. See [Table 17-4](#) for valid field options.

Step 2 From the Secondary Instances table, check the box the secondary instance that you want to promote to a primary instance.

Step 3 Click **Promote**.

The Distributed System Management page appears with the promoted instance.

Related Topics

- [Viewing and Editing a Secondary Instance, page 17-14](#)
- [Deleting a Secondary Instance, page 17-15](#)
- [Activating a Secondary Instance, page 17-15](#)
- [Deregistering Secondary Instances from the Distributed System Management Page, page 17-19](#)
- [Using the Deployment Operations Page to Create a Local Mode Instance, page 17-24](#)

Promoting a Secondary Instance from the Deployment Operations Page

To promote a secondary instance to a primary instance from the Deployment Operations page:

-
- | | |
|---------------|---|
| Step 1 | Choose System Administration > Operations > Distributed System Management .
The Deployment Operations page appears. See the Table 17-6 for valid field options. |
| Step 2 | Register the secondary instance to the primary instance. See Registering a Secondary Instance to a Primary Instance, page 17-16 . |
| Step 3 | Choose System Administration > Operations > Distributed System Management .
The Deployment Operations page appears. |
| Step 4 | Check the box the secondary instance that you want to promote to a primary instance. |
| Step 5 | Click Promote to Primary .
The Distributed System Management page appears with the promoted instance. |
-

Related Topics

- [Viewing and Editing a Secondary Instance, page 17-14](#)
- [Deleting a Secondary Instance, page 17-15](#)
- [Replicating a Secondary Instance from a Primary Instance, page 17-21](#)
- [Activating a Secondary Instance, page 17-15](#)
- [Deregistering Secondary Instances from the Distributed System Management Page, page 17-19](#)
- [Promoting a Secondary Instance from the Distributed System Management Page, page 17-20](#)
- [Using the Deployment Operations Page to Create a Local Mode Instance, page 17-24](#)

Replicating a Secondary Instance from a Primary Instance

You can use two different pages to replicate a secondary instance:

- [Replicating a Secondary Instance from the Distributed System Management Page, page 17-21](#)
- [Replicating a Secondary Instance from the Deployment Operations Page, page 17-22](#)



Note

For more information on replication, see [ACS 4.x and 5.8.1 Replication, page 1-2](#).

Replicating a Secondary Instance from the Distributed System Management Page



Note

All ACS appliances must be in sync with the AD domain clock.

To replicate a secondary instance:

-
- Step 1** Choose **System Administration > Operations > Distributed System Management**.
The Distributed System Management page appears.
- Step 2** From the Secondary Instances table, check one of check boxes the secondary instances that you want to replicate.
- Step 3** Click **Full Replication**.
The system displays the following warning message:
This operation will force a full replication for this secondary server. ACS will be restarted. You will be required to login again. Do you wish to continue?
- Step 4** Click **OK**.
- Step 5** Log into the ACS machine.
- Step 6** Choose **System Administration > Operations > Distributed System Management**.
The Distributed System Management page appears. On the Secondary Instance table, the Replication Status column shows **UPDATED**. Replication is complete on the secondary instance. Management and runtime services are current with configuration changes from the primary instance.
-

Replicating a Secondary Instance from the Deployment Operations Page



Note

All ACS appliances must be in sync with the AD domain clock.

To replicate a secondary instance:

-
- Step 1** Choose **System Administration > Operations > Local Operations > Deployment Operations**.
The Deployment Operations page appears. See the [Table 17-6](#) for valid field options.
- Step 2** Click **Force Full Replication**.
The system displays the following warning message:
This operation will force a full replication for this secondary server. ACS will be restarted. You will be required to login again. Do you wish to continue?
- Step 3** Click **OK**.
- Step 4** Log into the ACS machine.
- Step 5** Choose **System Administration > Operations > Distributed System Management**.
The Distributed System Management page appears. On the Secondary Instance table, the Replication Status column shows **UPDATED**. Replication is complete on the secondary instance. Management and runtime services are current with configuration changes from the primary instance.
-

Changing the IP address of a Primary Instance from the Primary Server

To change the IP address of a primary ACS server:

-
- Step 1** Log into the ACS primary web interface and Choose **System Administration > Operations > Distributed System Management** to deregister all the secondary ACS instances from the primary ACS server.
- The Distributed System Management page is displayed.
- Step 2** Check the check box near the secondary ACS instance one by one and click **Deregister**.
- Make sure that the log collector is running in the primary ACS server before deregistering all secondary ACS instances. If the log collector is running in any one of the secondary ACS server, change the log collector to the primary ACS server.
- To change the log collector, see [Configuring the Log Collector, page 18-36](#).
- Step 3** Check the check boxes near the deregistered secondary ACS instances to delete all deregistered secondary ACS instances.
- The deregistered secondary ACS instances are deleted.
- Step 4** Log into the ACS server in Admin mode by entering:
- ```
acs-5-2-a/admin# conf t
```
- Step 5** Enter the following commands:
- ```
int g 0
ip address old ip address new ip address
```
- Step 6** Press **Ctrl z**.
- The following warning message is displayed.
- ```
Changing the hostname or IP may result in undesired side effects, such as installed
application(s) being restarted.Are you sure you want to proceed? [y/n]
```
- Step 7** Press **y**
- Step 8** Access the primary ACS server using the administrator mode and the new IP address.
- Step 9** Use the command **show application status acs** to check if all process are running properly.
- Step 10** Register the secondary instances to the primary ACS server. See [Registering a Secondary Instance to a Primary Instance, page 17-16](#)
- 

## Failover

ACS 5.8.1 allows you to configure multiple ACS instances for a deployment scenario. Each deployment can have one primary and multiple secondary ACS servers.

Scenario: Primary ACS goes down in a Distributed deployment

Consider we have three ACS instances ACS1, ACS2, and ACS3.

ACS1 is the primary, and ACS2 and ACS3 are secondaries. You cannot make any configuration changes on the secondary servers when the primary server ACS1 is down. If all other secondary ACS servers are active, we can make any secondary server as a primary server.

- 
- Step 1** Promote the ACS2 to the primary for the time being and use it to make configuration changes.
- See [Promoting a Secondary Instance from the Distributed System Management Page, page 17-20](#) and [Promoting a Secondary Instance from the Deployment Operations Page, page 17-21](#) to promote a secondary ACS server as a primary server.
- Now, ACS2 is the new primary instance. So, we can make the configuration changes on ACS2 and it will be instantly replicated to ACS3 and on all secondary servers.
- Now, consider the ACS1 is back Online. If you need to retain the changes made on ACS2 and the rest of the deployment so that ACS1 is the standalone, do not replicate the changes anymore.
- Step 2** Delete ACS2 and ACS3 from the secondary server list of ACS1.
- Step 3** Delete ACS1 from ACS2, the current primary server to register ACS1 as secondary.
- Now, ACS2 is the primary server and ACS1 is the secondary server. The deployment is now completely back Online.
- If you want ACS1 to be the primary server, then you need to promote ACS1 as a primary server.
- 

## Using the Deployment Operations Page to Create a Local Mode Instance

When the secondary instance is in local mode it does not receive any configuration changes from the primary instance. The configuration changes you make to the secondary instance are local and do not propagate to the primary instance.

To use the Deployment Operations page to create a local mode instance:

- 
- Step 1** Choose **System Operations > Operations > Local Operations > Deployment Operations**.
- The Deployment Operations page appears. See the [Table 17-4 on page 10](#) for valid field options.
- Step 2** Specify the appropriate values in the Registration section for the secondary instance you want to register.
- Step 3** Click **Register to Primary**.
- The system displays the following warning message:
- This operation will register this ACS Instance as a secondary to the specified Primary Instance. ACS will be restarted. You will be required to login again. Do you wish to continue?
- Step 4** Click **OK**.
- Step 5** Log into the ACS local machine.
- Step 6** Choose **System Administration > Operations > Local Operations > Deployment Operations**.
- The Deployment Operations page appears.
- 4. Click Request Local Mode.**
- The secondary instance is now in local mode.
- After you reconnect the secondary instance to a primary instance you will lose the configuration changes you made to the local secondary instance. You must manually restore the configuration information for the primary instance.

You can use the configuration information on the ACS Configuration Audit report to manually restore the configuration information for this instance.

## Creating, Duplicating, Editing, and Deleting Software Repositories

To create, duplicate, edit, or delete a software repository:

**Step 1** Choose **System Administration > Operations > Software Repositories**.

The Software Repositories page appears with the information described in [Table 17-7](#):

**Table 17-7** *Software Repositories Page*

| Option           | Description                                                                                                                                                              |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name             | Name of the software repository.<br><b>Note</b> In ACS web interface, you cannot configure utf-8 characters for a backup filename and a repository name.                 |
| Protocol         | Name of the protocol (DISK, FTP, SFTP, TFTP, NFS) you want to use to transfer the upgrade file.                                                                          |
| Server Name      | Name of the server.                                                                                                                                                      |
| Path             | Name of the path for the directory containing the upgrade file. You must specify the protocol and the location of the upgrade file; for example, ftp://acs-home/updates. |
| Description      | Description of the software repository.                                                                                                                                  |
| Download RSA Key | Click this option to download the generated RSA public authentication key.                                                                                               |
| Generate RSA Key | Click this option to generate RSA public authentication key for SFTP repositories.                                                                                       |

**Step 2** Perform one of these actions:

- Click **Create**.
- Check the check box the software repository that you want to duplicate and click **Duplicate**.
- Click the software repository that you want to modify; or, check the check box for the name and click **Edit**.
- Check one or more check boxes the software repository that you want to delete and click **Delete**.

The Software Update Repositories Properties Page appears.

**Step 3** Complete the fields in the Software Repositories Properties Page as described in [Table 17-8](#):

**Table 17-8** *Software Update Repositories Properties Page*

| Option         | Description                                                                                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General</b> |                                                                                                                                                          |
| Name           | Name of the software repository.<br><b>Note</b> In ACS web interface, you cannot configure utf-8 characters for a backup filename and a repository name. |
| Description    | Description of the software repository.                                                                                                                  |

Table 17-8 Software Update Repositories Properties Page (continued)

| Option                                                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Repository Information</b>                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Protocol                                                                                          | The name of the protocol that you want to use to transfer the upgrade file. Valid options are: <ul style="list-style-type: none"> <li>DISK—If you choose this protocol, you must provide the path.</li> <li>FTP—If you choose this protocol, you must provide the server name, path, and credentials.</li> <li>SFTP—If you choose this protocol, you must provide the server name, path, and credentials.</li> <li>TFTP—If you choose this protocol, you must enter the name of the TFTP server. You can optionally provide the path.</li> <li>NFS—If you choose this protocol, you must provide the server name and path. You can optionally provide the credentials. If you choose this protocol, make sure that ACS has full access to the NFS file system. You must have read-write and allow root access permission on the NFS file system.</li> </ul> |
| Server Name                                                                                       | Name of the FTP, SFTP, TFTP, or NFS server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Note</b> The actual location that the repository points to is <code>/localdisk/pathname</code> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Path                                                                                              | Name of the path for the upgrade file. You must specify the protocol and the location of the upgrade file; for example, <code>ftp://acs-home/updates</code> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Enable RSA public key authentication                                                              | Check this check box if you want to use RSA public key for authentication against SFTP repositories. If you enable this option, you have to generate the RSA key from Software Repositories page and ACS uses the generated RSA key to connect to the SFTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>User Credentials</b>                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Username                                                                                          | Administrator name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Password                                                                                          | Administrator password.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Step 4** Click **Submit**.

The new software repository is saved. The Software Repository page appears, with the new software repository that you created, duplicated, or edited.

**Related Topics**

- [Managing Software Repositories from the Web Interface and CLI, page 17-26](#)

## Managing Software Repositories from the Web Interface and CLI

You can manage repositories from the web interface or the CLI. Keep in mind the rules for creating or deleting repositories from the web interface or CLI:

- If you create a repository from the CLI, that repository is not visible from the web interface, and can only be deleted from the CLI.
- If you create a repository from the web interface, it can be deleted from the CLI; however, that repository still exists in the web interface. If you use the web interface to create a repository for a software update, the repository is automatically created again in the CLI.
- If you delete a repository using the web interface, it is also deleted in the CLI.

## Configuring RSA Public Key for Authentication against SFTP Repositories

In general, when you want to configure an SFTP repository in ACS, you need to configure it with a username and password. The password of SFTP users are changing frequently according to the system requirement. Every time when there is a change in the user password, user needs to update the password in ACS repository configuration which is troublesome. To overcome this problem, ACS allows you to configure SFTP repository with RSA public key based authentication. In ACS 5.8.1, you can configure an SFTP repository with a username and RSA public key using which you can authenticate the users.

To configure SFTP repository with RSA Public key authentication, complete the following steps:

- 
- |               |                                                                                                                                                                                                                                                                               |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Login to ACS CLI.                                                                                                                                                                                                                                                             |
| <b>Step 2</b> | Configure an SFTP Repository with RSA public key authentication. For more information, see <a href="#">Configuring SFTP Repository in ACS CLI, page 17-27</a> .                                                                                                               |
| <b>Step 3</b> | Generate RSA Public key. You can generate RSA public key from ACS CLI and ACS web interface. For more information on generating RSA public key from ACS CLI, see <a href="#">Generating RSA Public Key, page 17-28</a> .                                                      |
| <b>Step 4</b> | Export the generated RSA public key to a remote repository. For more information on exporting RSA public key, see <a href="#">Exporting RSA Public Key to a remote Repository, page 17-28</a> .                                                                               |
| <b>Step 5</b> | Enable the RSA public key authentication in the SFTP server. For more information, see <a href="#">Enabling RSA Public Key Authentication in SFTP Repository, page 17-29</a> .                                                                                                |
| <b>Step 6</b> | Add the exported RSA public key to the authorized keys list on the SFTP server. For more information on adding the public key to the authorized keys list, see <a href="#">Adding the Exported RSA Public Key to the Authorized Key List in SFTP Repository, page 17-29</a> . |
- 

## Configuring SFTP Repository in ACS CLI

To configure SFTP repository in ACS CLI, complete the following steps.

- 
- |               |                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Login to ACS CLI.                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Step 2</b> | Enter <b>configure terminal</b> to enter the configuration mode.                                                                                                                                                                                                                                                                                                                                           |
| <b>Step 3</b> | Enter the <b>repository sftp</b> command to enter the configure repository mode.                                                                                                                                                                                                                                                                                                                           |
| <b>Step 4</b> | Enter the <b>url sftp: &lt;repository IP address&gt; /&lt;path&gt;</b> command where “repository IP address” is the IP address of the SFTP repository and the “path” is the path in which you are going to store the data in the SFTP repository.                                                                                                                                                          |
| <b>Step 5</b> | Perform one of the following actions: <ul style="list-style-type: none"><li>• Enter the <b>user &lt;username&gt; Password {hash \ plain} &lt;password&gt;</b> command to configure the repository password with username and password.</li><li>• Enter the <b>user &lt;username&gt; rsa-public-key</b> command to configure the SFTP repository with username and RSA public key authentication.</li></ul> |
| <b>Step 6</b> | Enter the <b>exit</b> command to come out of the repository configuration mode.<br>ACS CLI displays the following warning message.                                                                                                                                                                                                                                                                         |

% Warning: Host key of the server must be added using "crypto host\_key add" exec command before sftp repository can be used.

- Step 7** Enter the **exit** command to come out of the configuration mode.
- Step 8** Enter **show running-config** to see the configured RSA public key for sftp repository.
- 

## Generating RSA Public Key

You can generate RSA public key from both ACS CLI and ACS web interface.

### Generating RSA Public Key using ACS CLI

To generate RSA public key from ACS CLI, complete the following steps.

- Step 1** Login to ACS CLI.
- Step 2** Enter the **crypto key generate rsa passphrase <passphrase key>** command.
- Step 3** Press **Enter**.

The following message is displayed.

RSA key pair for user admin generated.

---

### Generating RSA Public Key using ACS web interface

To generate RSA public key from ACS web interface, complete the following steps.

- Step 1** Login to ACS web interface.
- Step 2** Choose **System Administration > Operations > Software Repositories**.
- Step 3** Click **Generate RSA Key**.
- Step 4** Enter the **Passphrase**.
- Step 5** Enter the same Passphrase again in the **Confirm Passphrase** field.
- Step 6** Click **OK**.

The RSA key is now generated.

---



#### Note

If you generate RSA public key from ACS web interface, then you need to download it using the **Download RSA Key** to add it to the authorized\_keys file in SFTP repository.

---

## Exporting RSA Public Key to a remote Repository

The SFTP repository is not functional yet. Therefore, you need to export the RSA public key file to a remote repository, copy the key file contents from the remote repository and add it to the SFTP repository authorized key file.

To export the RSA public key to a remote repository, complete the following steps.

- 
- Step 1** Login to ACS CLI.
- Step 2** Enter the **crypto key export <key\_file\_name> repository <repository\_name>** to export the generated RSA key to a remote repository.
- You can now open the remote repository to which the RSA public key is exported, copy it, and add it to the SFTP repository `authorized_keys` file.
- 

## Enabling RSA Public Key Authentication in SFTP Repository

To enable RSA public key authentication in SFTP repository, complete the following steps.

- 
- Step 1** Login to SFTP server with required permission to edit the `/etc/ssh/sshd_config` file.
- Step 2** Enter the **vi /etc/ssh/sshd\_config** command.
- SFTP server lists the contents of the `sshd_config` file.
- Step 3** Remove the “#” symbol from the following three lines to enable the RSA public key authentication.
- `RSAAuthentication yes`
  - `PubkeyAuthentication yes`
  - `AuthorizedKeysFile ~/.ssh/authorized_keys`
- RSA public key authentication is now enabled in this SFTP server.
- 

## Adding the Exported RSA Public Key to the Authorized Key List in SFTP Repository

To add the exported RSA public key to authorized keys file in SFTP repository, complete the following steps.

- 
- Step 1** Login to SFTP server with required permission to edit the `/etc/ssh/sshd_config` file.
- Step 2** Enter the **vi /home/<SFTP-username>/.ssh/authorized\_keys** command.
- This command opens the `authorized_keys` file from the home repository. If the `authorized_keys` file is not available, then SFTP repository creates a file on the same name.
- Step 3** Copy the contents from RSA public key file that you have exported to a remote repository and paste it in the `authorized_keys` file.
- Step 4** Enter “**wq!**” to save the `authorized_keys` file.
- The generated RSA public key is now added to the `authorized_keys` file in SFTP repository.
- 

### Related Topics

- [Creating, Duplicating, Editing, and Deleting Software Repositories, page 17-25](#)

# Exporting Policies from ACS Web Interface

ACS allows you to export the following policies and policy elements from the ACS web interface as an XML file to a remote repository or to email ids that you have configured:

- Service Selection Rules
- Access Services (Default Device Admin and Default Network Access)
- Group Mapping
- Authorization Policies
- Authorization Profiles
- Command Sets
- Shell Profiles
- Downloadable Access Lists

You can configure remote repositories in ACS from the Software Repositories page in ACS web interface. You can perform an instant export or schedule it for a future day and time from the ACS web interface. ACS exports the above mentioned policies and policy elements as an XML file and encrypts it with a password. ACS stores the exported XML file in the remote repository or sends an email to the recipients configured in the ACS web interface. You can decrypt the exported XML file using the encryption password to perform a quick analysis of the ACS configuration and identify any errors. You must have an administrator account with SuperAdmin role to export policies from the ACS web interface. ACS does not export Access Service policies of type Security Group Access and External Proxy.

## Before you Begin

Ensure that you have an administrator account with SuperAdmin role.

To export policies from the ACS web interface:

- 
- Step 1** Choose System **Administration > Operation > Scheduled Policy Export**.  
The Scheduled Policy Export properties page appears.
- Step 2** Complete the fields in the Scheduled Policy Export page as described in [Table 17-9](#):

**Table 17-9** *Scheduled Policy Export Page Properties*

| Option                                  | Description                                                                                                                                                                                                                                                                                   |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Export Policy Configuration Data</b> |                                                                                                                                                                                                                                                                                               |
| Encryption Password                     | Enter the password that ACS uses to encrypt the policies file that is being exported. You need to use this password to decrypt the exported XML file.                                                                                                                                         |
| Confirm Encryption Password             | Enter the password again which must match the encryption password entry exactly.                                                                                                                                                                                                              |
| Repository                              | Click <b>Select</b> to open the Software Update and Backup Repositories dialog box, from which you can select the appropriate repository in which you can store the exported policy file. You need to configure the remote repository in Software Repositories page on the ACS web interface. |
| Email file to                           | Enter the email address to which an email notification should be sent with the exported XML file. You can add multiple email addresses separating them with a comma.                                                                                                                          |



Table 17-9 Scheduled Policy Export Page Properties (continued)

| Option                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Mail Server             | Enter a valid IPv4 or IPv6 email host server. You will not receive an email if you do not configure the email server.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Schedule Options</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| On Demand Export        | Select if you want ACS to export the policies immediately after submitting the request (instant export).                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Schedule Export         | Select if you want ACS to schedule the export operation for a future day and time.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Time of Day             | Choose the time of the day at which you want ACS to export the policies. The export operation can be scheduled on a daily, weekly, or monthly basis. <ul style="list-style-type: none"> <li>• <b>Daily</b>—Choose this option to export the policies at the specified time every day.</li> <li>• <b>Weekly</b>—Choose this option and specify the day of the week to export policies every week on the specified day.</li> <li>• <b>Monthly</b>—Choose this option and specify the day of the month to export policies every month on the specified day.</li> </ul> |

**Step 3** Click **Submit**.

ACS exports the policies and policy elements:

- Immediately after submitting the request if you select the On Demand Export option.
- Saves the schedule and performs the export operation on the scheduled date and time if you select the Scheduled Export option.

**Related Topics**

[Creating, Duplicating, Editing, and Deleting Software Repositories, page 17-25](#)

## Trust Communication in a Distributed Deployment

ACS introduces the Trust Communication feature, which provides additional security for communication between the ACS instances in your deployment. You can use this feature to establish a secure tunnel for communication between the primary and secondary ACS instances in a deployment. You can enable Trust Communication on both the primary and secondary ACS instances or on either instance. However, for increased security, Cisco recommends that you enable Trust Communication on all nodes in your deployment. After the deployment is ready, you cannot edit the Enable Nodes Trust Communication settings on secondary ACS instances. The changes that you make in the Trust Communication settings of the primary ACS instance will be replicated to all secondary ACS instances.

In ACS 5.8.1, when you register a secondary instance to a primary instance, both the primary and secondary instances verify each other's certificates before establishing a secure tunnel for communication. All subsequent transactions between these two nodes happen through the established secure tunnel.

By default, Trust Communication is enabled on a fresh ACS instance. If you do not need this type of security, you can uncheck the **Enable Nodes Trust Communication** check box in the Trust Communication Settings page.

- When you enable Trust Communication on your primary and secondary ACS instance, and you register the secondary instance with the primary, both the primary and secondary instance check the CA and server certificates of each other. After the certificates are verified:
  - If the certificates in both the primary and secondary ACS instances are valid certificates, the instances establish a secure tunnel between them and register the secondary instance to the primary.
  - If any of the certificates in the primary instance are invalid, the secondary ACS instance stops the registration process.
  - If any of the certificates in the secondary instance are invalid, the primary ACS instance rejects the register request from the secondary ACS instance.
- When you enable Trust Communication only in the primary ACS instance and register a secondary to this primary, then this primary instance verifies the secondary's certificates. If the certificates are valid, the primary registers the new ACS instance as a secondary instance. The secondary does not verify the primary's certificates.
- When you enable Trust Communication only in the secondary ACS instance and register this instance to the primary instance, then this secondary instance verifies the primary's certificates during registration. If the certificates are valid, the secondary instance proceeds with the registration process. The primary instance does not verify the secondary's certificates.

**Note**

If the certificates that you have used for ACS instances in a deployment are invalid (such as expired certificates, revoked certificates, and not yet valid certificates), then the primary and secondary ACS instances cannot communicate and the system will not work as expected.

## Configuring Trust Communication in a Distributed Deployment

### Before You Begin

Before enabling Trust Communication between nodes in a distributed deployment, you need to make sure that you have done the following:

- Add a trusted Certificate Authority (CA) certificate in your Primary ACS instance. For more information, see [Adding a Certificate Authority, page 8-95](#).
- Add a management server certificate duly signed by a valid CA to the primary ACS instance. For more information, see [Configuring Local Server Certificates, page 18-16](#).
- Add a trusted CA to the ACS instance which is going to be registered as a secondary ACS instance. For more information, see [Adding a Certificate Authority, page 8-95](#).
- Add a management server certificate duly signed by a valid CA to the ACS instance that is going to be registered as a secondary ACS instance. For more information, see [Configuring Local Server Certificates, page 18-16](#).
- Make sure that the CA that issued the server certificate of the secondary instance is present in the primary instance and that the CA that issued the server certificate of the primary instance is present in the secondary instance.

To configure Trust Communication between nodes in a distributed deployment.

- Step 1** Choose **System Administration > Configuration > Global System Options > Trust Communication Settings**.

**Step 2** Check the **Enable Nodes Trust Communication** check box.

**Step 3** Click **Submit**.

Trust Communication between the nodes is enabled now. You can now register a secondary instance to the primary. For more information, see [Registering a Secondary Instance to a Primary Instance](#), page 17-16.

---





# Managing System Administration Configurations

---

After you install Cisco Secure ACS, you must configure and administer it to manage your network efficiently. The ACS web interface allows you to easily configure ACS to perform various operations. For a list of post-installation configuration tasks to get started with ACS, see [Post-Installation Configuration Tasks, page 6-1](#).

When you choose **System Administration > Configuration**, you can access pages that allow you do the following:

- Configure global system options, including settings for TACACS+, EAP-TLS, PEAP, and EAP-FAST. See [Configuring Global System Options, page 18-1](#).
- Configure protocol dictionaries. See [Managing Dictionaries, page 18-6](#).
- Manage local sever certificates. See [Configuring Local Server Certificates, page 18-16](#).
- Manage log configurations. See [Configuring Local and Remote Log Storage, page 18-23](#).
- Manage licensing. See [Licensing Overview, page 18-37](#).

## Configuring Global System Options

From the **System Administration > Configuration > Global System Options** pages, you can view these options:

- [Configuring TACACS+ Settings, page 18-1](#)
- [Configuring EAP-TLS Settings, page 18-2](#)
- [Configuring PEAP Settings, page 18-3](#)
- [Configuring HTTP Proxy Settings for CRL Requests, page 18-3](#)
- [Configuring EAP-FAST Settings, page 18-4](#)
- [Generating EAP-FAST PAC, page 18-4](#)
- [Generating EAP-FAST PAC, page 18-4](#)

## Configuring TACACS+ Settings

Use the TACACS+ Settings page to configure TACACS+ runtime characteristics.

Select **System Administration > Configuration > Global System Options > TACACS+ Settings**.

The TACACS+ Settings page appears as described in [Table 18-1](#):

**Table 18-1** *TACACS+ Settings*

| Option                         | Description                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port to Listen                 | Port number on which to listen. By default, the port number is displayed as 49. ACS 5.8.1 allows you to edit this field. You can configure the TACACS+ port with number 49 and numbers ranging from 1024 to 65535. However, ACS does not allow the port numbers that are already assigned to other ports. This operation restarts the ACS runtime and all registered instances. |
| Connection Timeout             | Number of minutes before the connection times out.                                                                                                                                                                                                                                                                                                                              |
| Session Timeout                | Number of minutes before the session times out.                                                                                                                                                                                                                                                                                                                                 |
| Maximum Packet Size            | Maximum packet size (in bytes).                                                                                                                                                                                                                                                                                                                                                 |
| Single Connect Support         | Check to enable single connect support.                                                                                                                                                                                                                                                                                                                                         |
| <b>Login Prompts</b>           |                                                                                                                                                                                                                                                                                                                                                                                 |
| Username Prompt                | Text string to use as the username prompt.                                                                                                                                                                                                                                                                                                                                      |
| Password Prompt                | Text string to use as the password prompt.                                                                                                                                                                                                                                                                                                                                      |
| <b>Password Change Control</b> |                                                                                                                                                                                                                                                                                                                                                                                 |
| Enable TELNET Change Password  | Choose this option if you want to provide an option to change password during a TELNET session.                                                                                                                                                                                                                                                                                 |
| Prompt for Old Password:       | Text string to use as the old password prompt.                                                                                                                                                                                                                                                                                                                                  |
| Prompt for New Password        | Text string to use as the new password prompt.                                                                                                                                                                                                                                                                                                                                  |
| Prompt for Confirm Password    | Text string to use as the confirm password prompt.                                                                                                                                                                                                                                                                                                                              |
| Disable TELNET Change Password | Choose this option if you do not want change password during a TELNET session.                                                                                                                                                                                                                                                                                                  |
| Message when Disabled          | Message that is displayed when you choose the Disable TELNET Change Password option.                                                                                                                                                                                                                                                                                            |

## Configuring EAP-TLS Settings

Use the EAP-TLS Settings page to configure EAP-TLS runtime characteristics.

Choose **System Administration > Configuration > Global System Options > EAP-TLS Settings**.

The EAP-TLS Settings page appears as described in [Table 18-2](#):

**Table 18-2** *EAP-TLS Settings*

| Option                        | Description                                                                                                                                                                                                                                                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General</b>                |                                                                                                                                                                                                                                                                                                                                            |
| Enable EAP-TLS Session Resume | Check this check box to support abbreviated reauthentication of a user who has passed full EAP-TLS authentication.<br><br>This feature provides reauthentication of the user with only an SSL handshake and without the application of certificates. EAP-TLS session resume works only within the specified EAP-TLS session timeout value. |

Table 18-2 EAP-TLS Settings (continued)

| Option                          | Description                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EAP-TLS Session Timeout         | Enter the number of seconds before the EAP-TLS session times out. The default value is 7200 seconds.                                                                       |
| <b>Stateless Session Resume</b> |                                                                                                                                                                            |
| Master Key Generation Period    | The value is used to regenerate the master key after the specified period of time. The default is one week.                                                                |
| Revoke                          | Click <b>Revoke</b> to cancel all previous master keys. This operation should be used with caution.<br>If the ACS node is a secondary node, the Revoke option is disabled. |

## Configuring PEAP Settings

Use the PEAP Settings page to configure PEAP runtime characteristics.

Choose **System Administration > Configuration > Global System Options > PEAP Settings**.

The PEAP Settings page appears as described in [Table 18-3](#):

Table 18-3 PEAP Settings

| Option                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Enable PEAP Session Resume | When checked, ACS caches 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, ACS uses the cached TLS session, resulting in faster PEAP performance and a lessened AAA server load.<br><br>You must specify a PEAP session timeout value for the PEAP session resume features to work. |
| PEAP Session Timeout       | Enter the number of seconds before the PEAP session times out. The default value is 7200 seconds.                                                                                                                                                                                                                                                                                                                                                           |
| Enable Fast Reconnect      | Check to allow a PEAP session to resume in ACS without checking user credentials when the session resume feature is enabled.                                                                                                                                                                                                                                                                                                                                |

### Related Topics

- [Generating EAP-FAST PAC, page 18-4](#)

## Configuring HTTP Proxy Settings for CRL Requests

ACS 5.8.1 introduces proxy settings for CRL downloads to proxy requests and responses from the CRL distribution server for greater security. ACS provides an option for administrators to enable the proxy settings on the HTTP Proxy Settings page for ACS to communicate with the CRL distribution server through the configured proxy server. The proxy server receives the request from ACS and forwards it to the CRL distribution server. The CRL distribution server, upon receiving the request from the proxy, processes it and forwards the CRLs to the proxy server. The proxy server receives the CRLs from the CRL distribution server and forwards them to ACS.

Use the HTTP Proxy Settings page to configure the HTTP Proxy for CRL requests from ACS.

Choose **System Administration > Configuration > Global System Options > HTTP Proxy Settings**.

The HTTP Proxy Settings page appears as described in [Table 18-3](#):

**Table 18-4** *HTTP Proxy Settings*

| Option            | Description                                                                                                                                                                                                                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General</b>    |                                                                                                                                                                                                                                                                                                                                                                         |
| Enable HTTP Proxy | Check the Enable HTTP Proxy check box for ACS to communicate with the CRL distribution URL through a proxy server.                                                                                                                                                                                                                                                      |
| Proxy Address     | Enter the proxy IP address or DNS-resolvable hostname to be used as a proxy server for retrieving CRLs from an external CRL distribution server. ACS communicates with the configured proxy server for CRL information. The proxy server forwards the request to the CRL distribution server URL. The proxy server receives the revocation list and forwards it to ACS. |
| Proxy Port        | Enter the port number through which the proxy traffic travels to and from ACS.                                                                                                                                                                                                                                                                                          |

#### Related Topics

[Adding a Certificate Authority, page 8-95](#)

## Configuring EAP-FAST Settings

Use the EAP-FAST Settings page to configure EAP-FAST runtime characteristics.

Choose **System Administration > Configuration > Global System Options > EAP-FAST > Settings**.

The EAP-FAST Settings page appears as described in [Table 18-5](#):

**Table 18-5** *EAP-FAST Settings*

| Option                              | Description                                                                                                                                                                                                                                           |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General</b>                      |                                                                                                                                                                                                                                                       |
| Authority Identity Info Description | User-friendly string that describes the ACS server that sends credentials to a client. The client can discover this string in the Protected Access Credentials Information (PAC-Info) Type-Length-Value (TLV). The default value is Cisco Secure ACS. |
| Master Key Generation Period        | The value is used to encrypt or decrypt and sign or authenticate PACs. The default is one week.                                                                                                                                                       |
| <b>Revoke</b>                       |                                                                                                                                                                                                                                                       |
| Revoke                              | Click <b>Revoke</b> to revoke all previous master keys and PACs. This operation should be used with caution.<br><br>If the ACS node is a secondary node, the Revoke option is disabled.                                                               |

## Generating EAP-FAST PAC

Use the EAP-FAST Generate PAC page to generate a user or machine PAC.

- Step 1** Choose **System Administration > Configuration > Global System Options > EAP-FAST > Generate PAC**.

The Generate PAC page appears as described in [Table 18-6](#):



**Table 18-6**      *Generate PAC*

| Option           | Description                                                                                                                                                                       |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Tunnel PAC       | Select to generate a tunnel PAC.                                                                                                                                                  |
| Machine PAC      | Select to generate a machine PAC.                                                                                                                                                 |
| Identity         | Specifies the username or machine name presented as the “inner username” by the EAP-FAST protocol. If the Identity string does not match that username, authentication will fail. |
| PAC Time To Live | Enter the equivalent maximum value in seconds, minutes, hours, days, weeks, months, and years. Enter a positive integer.                                                          |
| Password         | Enter the password.                                                                                                                                                               |

**Step 2**    Click **Generate PAC**.

## Configuring RSA SecurID Prompts

You can configure RSA prompts for an ACS deployment. The set of RSA prompts that you configure is used for all RSA realms and ACS instances in a deployment. To configure RSA SecurID Prompts:

- Step 1**    Choose **System Administration > Configuration > Global System Options > RSA SecurID Prompts**. The RSA SecurID Prompts page appears.
- Step 2**    Modify the fields described in [Table 18-7](#).

**Table 18-7**      *RSA SecurID Prompts Page*

| Option                   | Description                                                                                                                |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Passcode Prompt          | Text string to request for the passcode. The default value is “Enter PASSCODE:”.                                           |
| Next Token Prompt        | Text string to request for the next token. The default value is “Enter Next TOKENCODE:”.                                   |
| Choose PIN Type Prompt   | Text string to request the PIN type. The default value is “Do you want to enter your own pin?”.                            |
| Accept System PIN Prompt | Text string to accept the system-generated PIN. The default value is “ARE YOU PREPARED TO ACCEPT A SYSTEM-GENERATED PIN?”. |

For the two PIN entry prompts below, if the prompt contains the following strings, they will be substituted as follows:

- {MIN\_LENGTH}—will be replaced by the minimum PIN length configured for the RSA realm.
- {MAX\_LENGTH}—will be replaced by the maximum PIN length configured for the RSA realm.
- /x/—to cancel the new PIN procedure.

|                         |                                                                                           |
|-------------------------|-------------------------------------------------------------------------------------------|
| Alphanumeric PIN Prompt | Text string for requesting an alphanumeric PIN.                                           |
| Numeric PIN Prompt      | Text string for requesting a numeric PIN.                                                 |
| Re-Enter PIN Prompt     | Text string to request the user to re-enter the PIN. The default value is “Reenter PIN:”. |

**Step 3** Click **Submit** to configure the RSA SecurID Prompts.

---

## Managing Dictionaries

The following tasks are available when you select **System Administration > Configuration > Dictionaries**:

- [Viewing RADIUS and TACACS+ Attributes, page 18-6](#)
- [Configuring Identity Dictionaries, page 18-12](#)

## Viewing RADIUS and TACACS+ Attributes

The RADIUS and TACACS+ Dictionary pages display the available protocol attributes in these dictionaries:

- RADIUS (IETF)
- RADIUS (Cisco)
- RADIUS (Microsoft)
- RADIUS (Ascend)
- RADIUS (Cisco Airespace)
- RADIUS (Cisco Aironet)
- RADIUS (Cisco BBSM)
- RADIUS (Cisco VPN 3000)
- RADIUS (Cisco VPN 5000)
- RADIUS (Juniper)
- RADIUS (Nortel [Bay Networks])
- RADIUS (RedCreek)
- RADIUS (US Robotics)
- TACACS+

To view and choose attributes from a protocol dictionary, select **System Administration > Configuration > Dictionaries > Protocols**; then choose a dictionary.

The Dictionary page appears with a list of available attributes as shown in [Table 18-8](#):

**Table 18-8** *Protocols Dictionary Page*

| Option    | Description                 |
|-----------|-----------------------------|
| Attribute | Name of the attribute.      |
| ID        | (RADIUS only) The VSA ID.   |
| Type      | Data type of the attribute. |

**Table 18-8** *Protocols Dictionary Page (continued)*

| Option           | Description                                                                                                                                           |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Direction        | (RADIUS only) Specifies where the attribute is in use: in the request, in the response, or both. Single or bidirectional authentication.              |
| Multiple Allowed | (RADIUS only) Multiple attributes are allowed. Attributes that specify <i>multiple allowed</i> can be used more than once in one request or response. |

Use the arrows to scroll through the attribute list.

ACS 5.8.1 also supports RADIUS vendor-specific attributes (VSAs). A set of predefined RADIUS VSAs are available. You can define additional vendors and attributes from the ACS web interface. You can create, edit, or delete RADIUS VSAs.

After you have defined new VSAs, you can use them in policies, authorization profiles, and RADIUS token servers in the same way as predefined VSAs. For more information, see:

- [RADIUS VSAs, page B-6.](#)
- [Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes, page 18-7](#)

## Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes

Vendor-specific attributes (VSAs) allow vendors to create extensions to the RADIUS attributes. Vendors are assigned a specific vendor numbers. VSAs are attributes that contain subattributes. ACS 5.8.1 allows you to create, duplicate, and edit RADIUS VSAs.

To Create, edit, and duplicate RADIUS VSAs:

Some of the internally used attributes cannot be modified. You cannot modify an attribute's type if the attribute is used by any policy or policy element.

**Step 1** Choose **System Administration > Configuration > Dictionaries > Protocols > RADIUS VSA**.

**Step 2** Do one of the following:

- Click **Create**.
- Check the check box the RADIUS VSA that you want to duplicate, and click **Duplicate**.
- Check the check box the RADIUS VSA that you want to edit, and click **Edit**.

The RADIUS VSA page appears. Modify the fields as described in [Table 18-9](#).

**Table 18-9** *RADIUS VSA - Create, Duplicate, Edit Page*

| Option           | Description                                                                                                                             |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Attribute        | Name of the RADIUS VSA.                                                                                                                 |
| Description      | (Optional)<br>A brief description of the RADIUS VSA.                                                                                    |
| Vendor ID        | ID of the RADIUS vendor.                                                                                                                |
| Attribute Prefix | (Optional)<br>Prefix that you want to prepend to the RADIUS attribute so that all attributes for the vendor start with the same prefix. |

Table 18-9 RADIUS VSA - Create, Duplicate, Edit Page (continued)

| Option                             | Description                                                                                                                                                 |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Use Advanced Vendor Options</b> |                                                                                                                                                             |
| Vendor Length Field Size           | Vendor length field of 8 bits for specifying the length of the VSA. Choose the vendor length of the VSA. Valid options are 0 and 1. The default value is 1. |
| Vendor Type Field Size             | Vendor type field of 8 bits. Choose the vendor type of the VSA. Valid options are 1, 2, and 4. The default value is 1.                                      |

**Step 3** Click **Submit** to save the changes.

#### Related Topics

[Viewing RADIUS and TACACS+ Attributes, page 18-6](#)

## Importing RADIUS Vendors and Vendor-Specific Attributes

ACS 5.8.1 supports importing RADIUS vendors and RADIUS vendor-specific attributes (VSAs). In ACS 5.8.1, you have the option to import the RADIUS vendors and RADIUS VSAs from a text file. This text file is based on the Free RADIUS format. For more information on the Free RADIUS format, see <http://linux.die.net/man/5/dictionary>. The ACS 5.8.1 web interface provides you the option to download the Import template. You need to enter the vendor and its attributes in the same file.



#### Note

ACS supports A-Z, a-z, 0-9, -, \_, and / characters for use in the Import file.

Each RADIUS vendor should have a unique vendor ID. You cannot provide different IDs for the same vendor. Therefore, when you import vendors and VSAs, if the vendor name or attribute is already present in ACS, then the import operation fails with errors. In this case, you need to delete that particular vendor, or both the vendors and its attributes, and then re-import the file. ACS displays an appropriate error message and stops the import operation if the file format is wrong or any unsupported characters are present in the file.

**Figure 18-1** Example for RADIUS Vendor and VSAs in Free RADIUS File

```

3 # dictionary.cisco
4 #
5 # Accounting VSAs originally by
6 # "Marcelo M. Sosa Luones" <marcelo@sosa.com.ar>
7 #
8 # Version: Id
9 #
10 # For documentation on Cisco RADIUS attributes, see:
11 #
12 # http://www.cisco.com/univercd/cc/td/doc/product/access/aaa_serv/yapp_dev/vsaig3.htm
13 #
14 # For general documentation on Cisco RADIUS configuration, see:
15 #
16 # http://www.cisco.com/en/US/partner/tech/tk583/tk547/tsd_technology_support_sub-protocol_home.html
17 #
18 #
19 VENDOR Cisco 9
20 #
21 # Standard attribute
22 #
23 BEGIN-VENDOR Cisco
24 #
25 #
26 ATTRIBUTE cisco-av-bair 1 string
27 ATTRIBUTE cisco-aaa-port 2 string
28 #
29 #
30 # T.37 Store-and-Forward attributes.
31 #
32 ATTRIBUTE cisco-fax-account-id-origin 3 string
33 ATTRIBUTE cisco-fax-msg-id 4 string
34 ATTRIBUTE cisco-fax-pages 5 string
35 ATTRIBUTE cisco-fax-coverpage-flag 6 string
36 ATTRIBUTE cisco-fax-modem-time 7 string
37 ATTRIBUTE cisco-fax-connect-speed 8 string
38 ATTRIBUTE cisco-fax-recipient-count 9 string
39 ATTRIBUTE cisco-fax-process-abort-flag 10 string
40 ATTRIBUTE cisco-fax-dsn-address 11 string
41 ATTRIBUTE cisco-fax-dsn-flag 12 string
42 ATTRIBUTE cisco-fax-mdn-address 13 string

```

361422

The # key at the beginning of a line indicates that the line is a comment line. The keyword VENDOR at the beginning of a line indicates that the line has vendors. The keyword ATTRIBUTE at the beginning of a line indicates that the line has VSAs. The value of a VSA should start with the vendor name. For instance, if the vendor name is Cisco, then the attribute value is cisco-fax-message-id.

When an attribute is of the Enumeration type, you need to specify the Enumeration name and Enumeration ID in the Free RADIUS file.

Table 18-10 displays the attributes types that are supported in a Free RADIUS text file and their mapping with the attribute types in ACS.

**Table 18-10** Attributes Mapping Between Free RADIUS File and ACS

| Attribute Type in Free RADIUS File | Attribute Type in ACS Web Interface |
|------------------------------------|-------------------------------------|
| String                             | String                              |
| Octets                             | HexString                           |
| IP address                         | IPv4 address                        |
| Integer                            | Integer/Enumeration                 |

The edit operation, delete operation, directions, and multi-value attributes are not supported when you import RADIUS vendors and RADIUS VSAs. You need to manually perform these operations after importing the vendors and VSAs.

To import RADIUS vendors and RADIUS VSAs:

- Step 1** Choose **System Administration > Configuration > Dictionaries > Protocols > RADIUS VSA**.  
The RADIUS VSA page appears.
- Step 2** Click **Import**.  
The Import dialog box appears.

- Step 3** Click **Download Template** to download the import file template from the ACS web interface and save it to your client machine.
- Step 4** Enter the RADIUS vendors and RADIUS VSAs in the specified format and save them.
- Step 5** Click **Browse** to browse to the location of the Free RADIUS format file that has the RADIUS vendors and RADIUS VSAs and is ready to be imported.
- Step 6** Click **Start Import** to start the import operation.
- The RADIUS vendors and RADIUS VSAs are imported. ACS displays the log messages in a pop-up window.

#### Related Topics

[Viewing RADIUS and TACACS+ Attributes, page 18-6](#)

## Creating, Duplicating, and Editing RADIUS Vendor-Specific Subattributes

To create, duplicate, and edit RADIUS vendor-specific subattributes:

- Step 1** Choose **System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA**.
- You can alternatively choose the RADIUS VSA from the navigation pane.
- Step 2** Do one of the following:
- Click **Create** to create a subattribute for this RADIUS VSA.
  - Check the check box the RADIUS VSA that you want to duplicate, then click **Duplicate**.
  - Check the check box the RADIUS VSA that you want to edit, then click **Edit**.
  - Check the check box a RADIUS Vendor and click **Show Vendor Attributes** to view the VSAs of this Vendor.
- The RADIUS VSA subattribute create page appears.
- Step 3** Complete the fields described in [Table 18-11](#).

**Table 18-11** *Creating, Duplicating, and Editing RADIUS Subattributes*

| Option                      | Description                                                                                                                             |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <b>General</b>              |                                                                                                                                         |
| Attribute                   | Name of the subattribute. The name must be unique.                                                                                      |
| Description                 | (Optional) A brief description of the subattribute.                                                                                     |
| <b>RADIUS Configuration</b> |                                                                                                                                         |
| Vendor Attribute ID         | Enter the vendor ID field for the subattribute. This value must be unique for this vendor.                                              |
| Direction                   | Specifies where the attribute is in use: in the request, in the response, or both. Single or bidirectional authentication.              |
| Multiple Allowed            | Multiple attributes are allowed. Attributes that specify <i>multiple allowed</i> can be used more than once in one request or response. |

Table 18-11 Creating, Duplicating, and Editing RADIUS Subattributes (continued)

| Option                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Include attribute in the log   | Check this check box to include the subattribute in the log. For sensitive attributes, you can uncheck this check box so they are not logged.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Attribute Type</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Attribute Type                 | Type of the attribute. Valid options are: <ul style="list-style-type: none"> <li>String</li> <li>Unsigned Integer 32</li> <li>IPv4 Address</li> <li>HEX String</li> <li>Enumeration—If you choose this option, you must enter the ID-Value pair</li> </ul> You cannot use attributes of type HEX String in policy conditions.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| ID-Value                       | (Optional) <i>For the Enumeration attribute type only.</i> <ul style="list-style-type: none"> <li>ID—Enter a number from 0 to 999.</li> <li>Value—Enter a value for the ID.</li> <li>Click <b>Add</b> to add this ID-Value pair to the ID-Value table.</li> </ul> To edit, replace, and delete ID-Value pairs: <ul style="list-style-type: none"> <li>Select the ID-Value pair from the ID-Value table.</li> <li>Click <b>Edit</b> to edit the ID and Value fields. Edit the fields as required.</li> <li>Click <b>Add</b> to add a new entry after you modify the fields.</li> <li>Click <b>Replace</b> to replace the same entry with different values.</li> <li>Click <b>Delete</b> to delete the entry from the ID-Value table.</li> </ul> |
| <b>Attribute Configuration</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Add Policy Condition           | Check this check box to enter a policy condition in which this subattribute will be used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Policy Condition Display Name  | Enter the name of the policy condition that will use this subattribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Step 4** Click **Submit** to save the subattribute.

## Viewing RADIUS Vendor-Specific Subattributes

To view the attributes that are supported by a particular RADIUS vendor:

- Step 1** Choose **System Administration > Configuration > Dictionaries > Protocols > RADIUS > RADIUS VSA**.
- The RADIUS VSA page appears.
- Step 2** Check the check box the vendor whose attribute you want to view, then click **Show Vendor Attributes**.

The vendor-specific attributes and the fields listed in [Table 18-8](#) are displayed. You can create additional VSAs, and duplicate or edit these attributes. For more information, see [Creating, Duplicating, and Editing RADIUS Vendor-Specific Subattributes](#), page 18-10.

---

#### Related Topic

[Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes](#), page 18-7

## Configuring Identity Dictionaries

This section contains the following topics:

- [Creating, Duplicating, and Editing an Internal User Identity Attribute](#), page 18-12
- [Deleting an Internal User Identity Attribute](#), page 18-14
- [Creating, Duplicating, and Editing an Internal Host Identity Attribute](#), page 18-14
- [Creating, Duplicating, and Editing an Internal Host Identity Attribute](#), page 18-14
- [Deleting an Internal Host Identity Attribute](#), page 18-15

## Creating, Duplicating, and Editing an Internal User Identity Attribute

To create, duplicate, and edit an internal user identity attribute:

---

**Step 1** Select **System Administration > Configuration > Dictionaries > Identity > Internal Users**.

The Attributes list for the Internal Users page appears.

**Step 2** Perform one of these actions:

- Click **Create**.
- Check the check box the attribute that you want to duplicate and click **Duplicate**.
- Click the attribute name that you want to modify; or, check the check box for the name and click **Edit**.

The Identity Attribute Properties page appears.

**Step 3** Modify the fields in the Identity Attributes Properties page as required. See [Configuring Internal Identity Attributes](#), page 18-13 for field descriptions.

**Step 4** Click **Submit**.

The internal user attribute configuration is saved. The Attributes list for the Internal Users page appears with the new attribute configuration.

---

#### Related Topics

- [Deleting an Internal User Identity Attribute](#), page 18-14
- [Creating, Duplicating, and Editing an Internal Host Identity Attribute](#), page 18-14
- [Policies and Identity Attributes](#), page 3-17



## Configuring Internal Identity Attributes

Table 18-12 describes the fields in the internal `<users | hosts>` identity attributes.

**Table 18-12** Identity Attribute Properties Page

| Option                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General</b>        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Attribute             | Name of the attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Description           | Description of the attribute.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Attribute Type</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Attribute Type        | <p>(Optional) Use the drop-down list box to choose an attribute type. Valid options are:</p> <ul style="list-style-type: none"> <li>String—Populates the Maximum Length and Default Value fields in the page. When you select String as the attribute type and enter a non-null value for a user, the user is authenticated against the ID store with the name that matches the already set value, for the attribute that is shown in the user details (ACS-RESERVED-Authen-ID-Store).</li> <li>Unsigned Integer 32—Populates the Valid Range From and To fields in the page.</li> <li>IP Address—Populates the Default Value field in the page. This can be either IPv4 or IPv6 addresses.</li> <li>Boolean—Populates the Default Value check box in the page. When you set the value of the Boolean attribute as true, it overrides the global settings for the password expiration policy and deactivates the policy (ACS-RESERVED-Never-Expired).</li> <li>Date—Populates the Default Value field and calendar icon in the page.</li> <li>Enumeration—Populates the ID and Value fields and the Add, Edit, Replace, and Delete buttons.</li> </ul> |
| Maximum Length        | (Optional) <i>For the String attribute type only.</i> Enter the maximum length of your attribute. The valid range is from 1 to 256. (Default = 32)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Value Range           | <p>(Optional) <i>For the Unsigned Integer attribute type only.</i></p> <ul style="list-style-type: none"> <li>From—Enter the lowest acceptable integer value. The valid range is from 0 to <math>2^{31}-1</math> (2147483647). This value must be smaller than the Valid Range To value.</li> <li>To—Enter the highest acceptable integer value. The valid range is from 0 to <math>2^{31}-1</math> (2147483647). This value must be larger than the Valid Range From value.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Default Value         | <p>Enter the default value for the appropriate attribute:</p> <ul style="list-style-type: none"> <li>String—Up to the maximum length. (Follow the UTF-8 standard.) You can use the letters a to z, A to Z, and the digits 0 to 9.</li> <li>Unsigned Integer 32—An integer in the range from 0 to <math>2^{31}-1</math> (2147483647).</li> <li>IP Address —Enter the IP address you want to associate with this attribute, in this format: <ul style="list-style-type: none"> <li>IPv4 address—<i>x.x.x.x</i>, where <i>x.x.x.x</i> is the IPv4 address (no subnet mask)</li> <li>IPv6 address—<i>x:x:x:x:x:x:x:x</i>, where <i>x:x:x:x:x:x:x:x</i> is the IPv6 address (no subnet mask)</li> </ul> </li> <li>Date—Click the calendar icon to display the calendar pop-up and select a date.</li> <li>Boolean Value—Select True or False.</li> </ul>                                                                                                                                                                                                                                                                                                    |

Table 18-12 Identity Attribute Properties Page (continued)

| Option                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ID-Value                       | <p>(Optional) <i>For the Enumeration attribute type only.</i></p> <ul style="list-style-type: none"> <li>ID—Enter a number from 0 to 999.</li> <li>Value—Enter a value for the ID.</li> <li>Click <b>Add</b> to add this ID-Value pair to the ID-Value table.</li> </ul> <p>To edit, replace, and delete ID-Value pairs:</p> <ul style="list-style-type: none"> <li>Select the ID-Value pair from the ID-Value table.</li> <li>Click <b>Edit</b> to edit the ID and Value fields. Edit the fields as required.</li> <li>Click <b>Add</b> to add a new entry after you modify the fields.</li> <li>Click <b>Replace</b> to replace the same entry with different values.</li> <li>Click <b>Delete</b> to delete the entry from the ID-Value table.</li> </ul> |
| <b>Attribute Configuration</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Mandatory Fields               | Check the check box to make this attribute a requirement in the User Properties page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Add Policy Condition           | Check the check box to create a custom condition from this attribute. When you check this option, you must enter a name in the Policy Condition Display Name field.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Policy Condition Display Name  | Enter a name for the policy condition. After you submit this page, the condition appears in the <b>Policy Elements &gt; Session Conditions &gt; Custom</b> page.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

## Deleting an Internal User Identity Attribute

To delete an internal user identity attribute:

- 
- Step 1** Select **System Administration > Configuration > Dictionaries > Identity > Internal Users**.  
The Attributes list for the internal user page appears.
- Step 2** Check the check box of the attribute you want to delete.  
Because deleting an identity attribute can take a long time to process, you can delete only one attribute at a time.
- Step 3** Click **Delete**.
- Step 4** For confirmation, click **OK** or **Cancel**.  
The Attributes list for the internal user page appears without the deleted attribute.
- 

### Related Topics

- [Creating, Duplicating, and Editing an Internal User Identity Attribute, page 18-12](#)
- [Policies and Identity Attributes, page 3-17](#)

## Creating, Duplicating, and Editing an Internal Host Identity Attribute

To create, duplicate, and edit an internal host identity attribute:

- 
- Step 1** Select **System Administration > Configuration > Dictionaries > Identity > Internal Hosts**.  
The Attributes list for the Internal Hosts page appears.
- Step 2** Do one of the following:
- Click **Create**.
  - Check the check box the attribute that you want to duplicate and click **Duplicate**.
  - Click the attribute name that you want to modify; or, check the check box for the name and click **Edit**.
- The Identity Attribute Properties page appears.
- Step 3** Modify the fields in the Identity Attributes Properties page as required. See [Table 18-12](#) for field descriptions.
- Step 4** Click **Submit**.  
The internal host attribute configuration is saved. The Attributes list for the Internal Hosts page appears with the new attribute configuration.
- 

**Related Topics**

- [Deleting an Internal Host Identity Attribute, page 18-15](#)
- [Policies and Identity Attributes, page 3-17](#)

## Deleting an Internal Host Identity Attribute

To delete an internal host identity attribute:

- 
- Step 1** Select **System Administration > Configuration > Dictionaries > Identity > Internal User**.  
The Attributes list for the Internal Hosts page appears.
- Step 2** Check the check box the attribute you want to delete.  
Because deleting an attribute can take a long time to process, you can delete only one attribute at a time.
- Step 3** Click **Delete**.
- Step 4** For confirmation, click **OK** or **Cancel**.  
The Attributes list for the Internal Hosts page appears without the deleted attribute.
- 

**Related Topics**

- [Creating, Duplicating, and Editing an Internal Host Identity Attribute, page 18-14](#)
- [Policies and Identity Attributes, page 3-17](#)

## Adding Static IP address to Users in Internal Identity Store

To add static IP address to a user in Internal Identity Store:

- 
- Step 1** Add a static IP attribute to internal user attribute dictionary:
- Step 2** Select **System Administration > Configuration > Dictionaries > Identity > Internal Users**.
- Step 3** Click **Create**.
- Step 4** Add static IP attribute.
- Step 5** Select **Users and Identity Stores > Internal Identity Stores > Users**.
- Step 6** Click **Create**.
- Step 7** Edit the static IP attribute of the user.
- 

## Configuring Local Server Certificates

Local server certificates are also known as ACS server certificates. ACS uses the local server certificates to identify itself to the clients. The local server certificates are used by:

- EAP protocols that use SSL/TLS tunneling.
- Management interface to authenticate the web interface (GUI).

This section contains the following topics:

- [Adding Local Server Certificates, page 18-16](#)
- [Importing Server Certificates and Associating Certificates to Protocols, page 18-17](#)
- [Generating Self-Signed Certificates, page 18-18](#)
- [Generating a Certificate Signing Request, page 18-19](#)
- [Binding CA Signed Certificates, page 18-20](#)
- [Editing and Renewing Certificates, page 18-20](#)
- [Deleting Certificates, page 18-21](#)
- [Exporting Certificates, page 18-22](#)
- [Viewing Outstanding Signing Requests, page 18-22](#)

## Adding Local Server Certificates

You can add a local server certificate, also known as an ACS server certificate, to identify the ACS server to clients.

- 
- Step 1** Select **System Administration > Configuration > Local Server Certificates > Local Certificates**.  
The Local Certificates page appears displaying the information in [Table 18-13](#):

**Table 18-13**      *Local Certificates Page*

| Option                | Description                                                                                       |
|-----------------------|---------------------------------------------------------------------------------------------------|
| Friendly Name         | Name that is associated with the certificate.                                                     |
| Issued To             | Entity to which the certificate is issued. The name that appears is from the certificate subject. |
| Issued By             | Trusted party that issued the certificate.                                                        |
| Valid From            | Date the certificate is valid from.                                                               |
| Valid To (Expiration) | Date the certificate is valid to.                                                                 |
| Protocol              | Protocol associated with the certificate.                                                         |

**Step 2**      Click **Add**.

**Step 3**      Enter the information in the Local Certificate Store Properties page as described in [Table 18-14](#):

**Table 18-14**      *Local Certificate Store Properties Page*

| Option                               | Description                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Import Server Certificate            | Select to browse the client machine for the Local Certificate file and import the private key and private key password. See <a href="#">Importing Server Certificates and Associating Certificates to Protocols</a> , page 18-17.<br><br>Supported certificate formats include CER, DER, PEM, or Microsoft private key proprietary format. |
| Generate Self Signed Certificate     | Select to generate a self-signed certificate. See <a href="#">Generating Self-Signed Certificates</a> , page 18-18.                                                                                                                                                                                                                        |
| Generate Certificate Signing Request | Select to generate a certificate signing request. See <a href="#">Generating a Certificate Signing Request</a> , page 18-19.                                                                                                                                                                                                               |
| Bind CA Signed Certificate           | Select to bind the CA certificate. After the RA signs the request, you can install the returned signed certificate on ACS and bind the certificate with its corresponding private key. See <a href="#">Binding CA Signed Certificates</a> , page 18-20.                                                                                    |

## Importing Server Certificates and Associating Certificates to Protocols

The supported certificate formats are either DER or PEM.

**Step 1**      Select **System Administration > Configuration > Local Server Certificates > Local Certificates > Add**.

**Step 2**      Select **Import Server Certificate > Next**.

**Step 3**      Enter the information in the ACS Import Server Certificate as described in [Table 18-15](#):

**Table 18-15** *Import Server Certificate Page*

| Option                       | Description                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Certificate File             | Select to browse the client machine for the local certificate file.                                                                |
| Private Key File             | Select to browse to the location of the private key.                                                                               |
| Private Key Password         | Enter the private key password. The value may be minimum length = 0 and maximum length = 256.                                      |
| <b>Protocol</b>              |                                                                                                                                    |
| EAP                          | Check to associate the certificate with EAP protocols that use SSL/TLS tunneling: EAP-TLS, EAP-FAST, and PEAP.                     |
| Management Interface         | Check to associate the certificate with the management interface.                                                                  |
| Allow Duplicate Certificates | Allows to add certificate with same CN and same SKI with different Valid From, Valid To, and Serial number.                        |
| <b>Override Policy</b>       |                                                                                                                                    |
| Replace Certificate          | Check to replace the content of an existing certificate with the one that you import, but retain the existing protocol selections. |

**Step 4** Click **Finish**.

The new certificate is saved. The Local Certificate Store page appears with the new certificate.

## Generating Self-Signed Certificates

**Step 1** Select **System Administration > Configurations > Local Server Certificates > Local Certificates > Add**.

**Step 2** Select **Generate Self Signed Certificate > Next**.

**Step 3** Enter the information in the ACS Import Server Certificate as described in [Table 18-16](#):

**Table 18-16** *Generate Self Signed Certificate*

| Option              | Description                                                                                                                                                                                                            |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Certificate Subject | Certificate subject entered during generation of this request. The Certificate Subject field may contain alphanumeric characters. The maximum number of characters is 1024. This field is prefixed with "cn=".         |
| Key Length          | Key length entered during generation of this request. Values may be 512, 1024, 2048, or 4096. If you are deploying ACS as a FIPS-compliant policy management-engine, you must specify a 2048-bit or larger key length. |
| Digest to Sign with | Select either SHA1 or SHA256 as management certificates, from the dropdown list.                                                                                                                                       |
| Expiration TTL      | Select the maximum value in days, weeks, months, and years, and enter a positive integer.                                                                                                                              |
| <b>Protocol</b>     |                                                                                                                                                                                                                        |
| EAP                 | Check to associate the certificate with EAP protocols that use SSL/TLS tunneling: EAP-TLS, EAP-FAST, and PEAP.                                                                                                         |

**Table 18-16**      *Generate Self Signed Certificate*

| Option                       | Description                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Management Interface         | Check to associate the certificate with the management interface.                                                                  |
| Allow Duplicate Certificates | Allows to add certificate with same CN and same SKI with different Valid From, Valid To, and Serial number.                        |
| <b>Override Policy</b>       |                                                                                                                                    |
| Replace Certificate          | Check to replace the content of an existing certificate with the one that you import, but retain the existing protocol selections. |

**Step 4**    Click **Finish**.

The new certificate is saved. The Local Certificate Store page appears with the new certificate.

## Generating a Certificate Signing Request

**Step 1**    Select **System Administration > Configurations > Local Server Certificates > Local Certificates > Add**.

**Step 2**    Select **Generate Certificate Signing Request > Next**.

**Step 3**    Enter the information in the ACS Import Server Certificate as described in [Table 18-17](#):

**Table 18-17**      *Generate Signing Requests*

| Option              | Description                                                                                                                                                                                                                                            |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Certificate Subject | Certificate subject entered during generation of this request. The Certificate Subject field may contain alphanumeric characters. The maximum number of characters is 1024. This field is prefixed with "cn=".                                         |
| Key Length          | Key length entered during generation of this request. Values may be 512, 1024, 2048, or 4096. If ACS is set to operate in FIPS mode, the certificate RSA key size must be 2048 bits or greater in size and use either SHA-1 or SHA-256 hash algorithm. |
| Digest to Sign with | Select either SHA1 or SHA256 as management certificates, from the dropdown list.                                                                                                                                                                       |

**Step 4**    Click **Finish**.

The following message is displayed:

A server certificate signing request has been generated and can be viewed in the "Outstanding Signing Requests" list.

The new certificate is saved. The Local Certificate Store page appears with the new certificate.

## Binding CA Signed Certificates

Use this page to bind a CA signed certificate to the request that was used to obtain the certificate from the CA.

- 
- Step 1** Select **System Administration > Configurations > Local Server Certificates > Local Certificates > Add**.
- Step 2** Select **Bind CA Signed Certificate > Next**.
- Step 3** Enter the information in the ACS Import Server Certificate as described in [Table 18-18](#):

**Table 18-18**      *Bind CA Signed Certificate*

| Option                       | Description                                                                                                                        |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| Certificate File             | Browse to the client machine and select the certificate file to be imported.                                                       |
| <b>Protocol</b>              |                                                                                                                                    |
| EAP                          | Check to associate the certificate with EAP protocols that use SSL/TLS tunneling: EAP-TLS, EAP-FAST, and PEAP.                     |
| Management Interface         | Check to associate the certificate with the management interface.                                                                  |
| Allow Duplicate Certificates | Allows to add certificate with same CN and same SKI with different Valid From, Valid To, and Serial number.                        |
| <b>Override Policy</b>       |                                                                                                                                    |
| Replace Certificate          | Check to replace the content of an existing certificate with the one that you import, but retain the existing protocol selections. |

- Step 4** Click **Finish**.

The new certificate is saved. The Local Certificate Store page appears with the new certificate.

---

### Related Topics

- [Configuring Local Server Certificates, page 18-16](#)
- [Certificate-Based Network Access, page 4-10](#)

## Editing and Renewing Certificates

You can renew an existing self-signed certificate without having to remove it and adding a new certificate. This ensures that any service that uses the local certificate continues without any interruption. To renew or extend a local server certificate:

1. Select **System Administration > Configuration > Local Server Certificates > Local Certificates**.
2. Click the name that you want to modify; or, check the check box for the Name, and click **Edit**.
3. Enter the certificate properties as described in [Table 18-19](#):



Table 18-19 Edit Certificate Store Properties Page

| Option                               | Description                                                                                                                                                                                                                                                  |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Issuer</b>                        |                                                                                                                                                                                                                                                              |
| Friendly Name                        | Name that is associated with the certificate.                                                                                                                                                                                                                |
| <b>Description</b>                   | Description of the certificate.                                                                                                                                                                                                                              |
| Issued To                            | <i>Display only.</i> The entity to which the certificate is issued. The name that appears is from the certificate subject.                                                                                                                                   |
| Issued By                            | <i>Display only.</i> The certification authority that issued the certificate.                                                                                                                                                                                |
| Valid From                           | <i>Display only.</i> The start date of the certificate's validity. An X509 certificate is valid only from the start date to the end date (inclusive).                                                                                                        |
| Valid To (Expiration)                | <i>Display only.</i> The last date of the certificate's validity.                                                                                                                                                                                            |
| Serial Number                        | <i>Display only.</i> The serial number of the certificate.                                                                                                                                                                                                   |
| <b>Protocol</b>                      |                                                                                                                                                                                                                                                              |
| EAP                                  | Check for ACS to use the local certificate with EAP protocols that use SSL/TLS tunneling: EAP-TLS, EAP-FAST, and PEAP.                                                                                                                                       |
| Management Interface                 | Check for ACS to use the local certificate for SSL client authentication.                                                                                                                                                                                    |
| <b>Renew Self Signed Certificate</b> |                                                                                                                                                                                                                                                              |
| Certificate Expires On               | <i>Display only.</i> Date the certificate expires.                                                                                                                                                                                                           |
| Renew Self Signed Certificate        | Check to allow the renewal of a self signed certificate that expired.                                                                                                                                                                                        |
| Expiration TTL                       | Expiration TTL is the number of days, months, weeks, or years that you want to extend the existing certificate for. Valid options are: one day, one month, one week, and one year.<br>At a maximum, you can extend the certificate for a period of one year. |

- Click **Submit** to extend the existing certificate's validity.  
The Local Certificate Store page appears with the edited certificate.

**Related Topic**

- [Configuring Local Server Certificates, page 18-16](#)

## Deleting Certificates

To delete a certificate:

- Step 1** Select **System Administration > Configuration > Local Server Certificates > Local Certificates**.
- Step 2** Check one or more check boxes the certificates that you want to delete.
- Step 3** Click **Delete**.
- Step 4** For confirmation, click **Yes** or **Cancel**.

The Certificate Store page appears without the deleted certificate(s).

#### Related Topic

- [Configuring Local Server Certificates, page 18-16](#)

## Exporting Certificates

To export a certificate:

- 
- Step 1** Select **System Administration > Configuration > Local Server Certificates > Local Certificates**.
- Step 2** Check the box the certificates that you want to export, then click **Export**.  
The Export Certificate dialog box appears.
- Step 3** Select one of the following options:
- Export Certificate Only
  - Export Certificate and Private Key
- Step 4** Enter your private key password in the Private Key Password field.
- Step 5** Enter the same password in the Confirm Password field.



**Note** Exporting the private key is not a secure operation and could lead to possible exposure of the private key.

- Step 6** Click **OK** or **Cancel**.
- 

#### Related Topic

- [Configuring Local Server Certificates, page 18-16](#)

## Viewing Outstanding Signing Requests

- 
- Step 1** Select **System Administration > Configurations > Local Server Certificates > Outstanding Signing Request**.

The Certificate Signing Request page appears displaying the information described in [Table 18-20](#):

**Table 18-20**      *Certificate Signing Request Page*

| Option              | Description                                                                                                                                                                                                                      |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                | Name of the certificate.                                                                                                                                                                                                         |
| Certificate Subject | Certificate subject entered during generation of this request. The Certificate Subject field may contain alphanumeric characters. The maximum number of characters is 1024. This field should automatically prefixed with “cn=”. |

*Table 18-20 Certificate Signing Request Page*

| Option        | Description                                                                                   |
|---------------|-----------------------------------------------------------------------------------------------|
| Key Length    | Key length entered during generation of this request. Values may be 512, 1024, 2048, or 4096. |
| Timestamp     | Date certificate was created.                                                                 |
| Friendly Name | Name that is associated with the certificate.                                                 |

**Step 2** Click **Export** to export the local certificate to a client machine.

## Configuring Local and Remote Log Storage

Log records are generated for:

- Accounting messages
- AAA audit and diagnostics messages
- System diagnostics messages
- Administrative and operational audit messages

The messages are arranged in tree hierarchy structure within the logging categories (see [Configuring Logging Categories, page 18-28](#) for more information).

You can store log messages locally or remotely, based on the logging categories and available disk spaces.

This section contains the following topics:

- [Configuring Remote Log Targets, page 18-23](#)
- [Configuring the Local Log, page 18-27](#)
- [Configuring Logging Categories, page 18-28](#)
- [Configuring Global Logging Categories, page 18-28](#)
- [Configuring Per-Instance Logging Categories, page 18-33](#)
- [Displaying Logging Categories, page 18-35](#)
- [Configuring the Log Collector, page 18-36](#)
- [Viewing the Log Message Catalog, page 18-36](#)

See [Understanding Logging, page A-1](#) for a description of the preconfigured global ACS logging categories and the messages that each contains.

## Configuring Remote Log Targets

You can configure specific remote log targets (on a syslog server only) to receive the logging messages for a specific logging category. See [Understanding Logging, page A-1](#) for more information on remote log targets. See [Configuring Logging Categories, page 18-28](#), for more information on the preconfigured ACS logging categories. ACS 5.8.1 allows you to send secure syslog messages to a remote log target. If you choose the secure syslog option, ACS logs the following messages in the System Diagnostic reports.

- Remote syslog target is unavailable.
- Remote syslog target connection is resumed.
- Remote syslog target buffer is cleared.

To create a new remote log target:

**Step 1** Choose **System Administration > Configuration > Log Configuration > Remote Log Targets**.

The Remote Log Targets page appears.

**Step 2** Do one of the following:

- Click **Create**.
- Check the check box the remote log target that you want to duplicate and click **Duplicate**.
- Click the name of the remote log target that you want to modify; or check the check box the name of the remote log target that you want to modify and click **Edit**.
- One of these pages appears:
- Remote Log Targets > Create, if you are creating a new remote log target.
- Remote Log Targets > Duplicate: “*log\_target*”, where *log-target* is the name of the remote log target you selected in [Step 2](#), if you are duplicating a remote log target.
- Remote Log Targets > Edit: “*log\_target*”, where *log-target* is the name of the remote log target that you selected in [Step 2](#), if you are modifying a remote log target.

**Step 3** Complete the required fields as described in [Table 18-21](#):

**Table 18-21** Remote Log Targets Configuration Page

| Option                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>General</b>              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Name                        | Name of the remote log target. Maximum name length is 32 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Description                 | Description of the remote log target. Maximum description length is 1024 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Type                        | Type of remote log target—Syslog (the only option).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Target Configuration</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| IP Address                  | IP address of the remote log target, in the format <i>x.x.x.x</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Target Type                 | Select the type of syslog target type. By default it is set to UDP Syslog. The available target types are: <ul style="list-style-type: none"> <li>• UDP Syslog—The log messages are sent to the remote syslog target over a UDP connection.</li> <li>• TCP Syslog—The log messages are sent to the remote syslog target over a TCP connection.</li> <li>• Secure TCP Syslog—The log messages are sent to the remote syslog target over a secure TCP connection. The administrator has to configure CA and server certificates in both ACS and the remote syslog target. ACS verifies the server certificates from the remote syslog server and if the certificates are valid, it establishes a secure TCP connection between ACS and the remote syslog target to send the log messages.</li> </ul> |
| Use Advanced Syslog Options | Click to enable the advanced syslog options—port number, facility code, maximum length, buffer messages when server down, buffer size, reconnect timeout, select certificate authority, accept any syslog server. ACS displays the Advanced Syslog Options according to the selected target type.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

Table 18-21 Remote Log Targets Configuration Page

| Option                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port                             | <p>Port number of the remote log target used as the communication channel between the ACS and the remote log target.</p> <ul style="list-style-type: none"> <li>The default port number for UDP Syslog is 514.</li> <li>The default port number for TCP Syslog is 1468.</li> <li>The default port number for Secure TCP Syslog is 6514.</li> </ul>                                                                                                                                                                                        |
| Facility Code                    | <p>Facility code. Valid options are:</p> <ul style="list-style-type: none"> <li>LOCAL0 (Code = 16)</li> <li>LOCAL1 (Code = 17)</li> <li>LOCAL2 (Code = 18)</li> <li>LOCAL3 (Code = 19)</li> <li>LOCAL4 (Code = 20)</li> <li>LOCAL5 (Code = 21)</li> <li>LOCAL6 (Code = 22; default)</li> <li>LOCAL7 (Code = 23)</li> </ul>                                                                                                                                                                                                                |
| Maximum Length                   | Maximum length of the remote log target messages. Valid options are from 200 to 8192. The default value is 1024.                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Buffer Messages When Server Down | Check this check box if you want ACS to buffer the syslog messages when the TCP syslog targets and secure syslog targets are unavailable. ACS retries sending the messages to the target when the connection is re-established. After the connection is re-established, messages are sent in 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                      | <p>(Required only when you check the Buffer Messages When Server Down check box.) Maximum size (in MB) of the buffer messages that can be stored in ACS when the remote syslog server is down. By default, it is set to 100 MB. The valid range is from 10 to 100 MB. Changing the buffer size clears the buffer and all existing buffered messages for the specific target are lost.</p> <p>These buffer messages are cleared when you edit some of the options in the Remote Log Targets page. See the note below for more details.</p> |
| Reconnect Timeout                | <p>(Applicable only for TCP Syslog and Secure TCP Syslog targets.)</p> <p>The time interval at which ACS tries to reconnect to the remote syslog server when the remote syslog server is down and disconnected from ACS. The valid range is from 30 to 120 seconds. The default value is 30 seconds.</p>                                                                                                                                                                                                                                  |
| Select Certificate Authority     | <p>(Required only for Secure TCP Syslog targets.)</p> <p>The administrator have to choose one of the installed CA certificates in the CTL to be used for Secure Syslog. ACS tries to find a first valid local certificate that was signed by the selected CA for TLS negotiation with the syslog server. The administrator cannot choose the specific certificate. If ACS cannot find a valid installed local certificate, it uses the management certificate.</p>                                                                        |
| Accept Any SysLog Server         | <p>(Applicable only for Secure TCP Syslog targets.)</p> <p>Check this check box if you want ACS to ignore server certificate validation and accept any syslog server. By default, this option is unchecked. This option is disabled when you run ACS in FIPS mode.</p> <p><b>Note</b> You must uncheck this option if ACS is set to operate in FIPS mode.</p>                                                                                                                                                                             |

**Step 4** Click **Submit**.

The remote log target configuration is saved. The Remote Log Targets page appears with the new remote log target configuration.

**Note**

- When you edit the IP Address, Target Type, Buffer Size, Maximum Length, or Port fields of a remote log target, ACS displays the following message in a pop up window:  
Your changes will delete all not sent messages in buffer. Do you want to continue?  
You can click **OK** to delete the buffer messages and save the changes made in the fields. Click **Cancel** if you do not want to delete the buffer messages.
- When you use multiple remote log targets for an ACS instance and edit the IP Address, Target Type, Buffer Size, Maximum Length, or Port fields of a remote log target, the buffer messages specific only to the edited remote log target are deleted. This operation does not affect the buffer messages that are associated with the unedited other remote log targets.
- When a remote log target of an ACS deployment goes down, ACS stores the log messages in the relevant instance's buffer. For example, if the log message is created in the primary instance, ACS stores the messages in the primary instance's buffer. If the log message is created in the secondary instances, ACS stores the messages in the corresponding secondary instance's buffer.
- In an ACS deployment, the server certificate issued by the remote log target's CA should be installed in all ACS instances.
- When you select Secure TCP as the target type for a remote log target, the log collector acts as both the syslog server and the client (internal communication is through SSL). In this case, the root CA that has issued the log collector's management certificate must be installed in the CA trust list for the SSL handshake to be successful.
- If the management certificate of the log collector has Key Usage (KU), Enhanced Key Usage (EKU), and Netscape certificate type fields, then both the server and client authentication details must be set in these fields where as the other ACS instances in the deployment must have only the client authentication details.
- To send all CARS related log messages to the remote syslog server, execute the **logging <syslog ip>** command from ACS CLI. After executing this command, ACS does not send CARS related messages to the log collector server.

**Related Topic**

- [Deleting a Remote Log Target, page 18-26](#)

## Deleting a Remote Log Target

To delete a remote log target:

**Step 1** Select **System Administration > Configuration > Log Configuration > Remote Log Targets**.

The Remote Log Targets page appears, with a list of configured remote log targets.

**Step 2** Check one or more check boxes the remote log targets you want to delete.**Step 3** Click **Delete**.

The following error message appears:

Are you sure you want to delete the selected item/items?

**Step 4** Click **OK**.

The Remote Log Targets page appears without the deleted remote log targets.

---

#### Related Topic

- [Configuring Remote Log Targets, page 18-23](#)

## Configuring the Local Log

Use the Local Configuration page to configure the maximum days to retain your local log data.

---

**Step 1** Select **System Administration > Configuration > Log Configuration > Local Log Target**.

The Local Configuration page appears.

**Step 2** In the Maximum log retention period box, enter the number of days for which you want to store local log message files, where *<num>* is the number of days you enter. Valid options are 1 to 365. (Default = 7.)



**Note** If you reduce the number of days for which to store the local log message files, the log message files older than the number of days you specify are deleted automatically.

---

You can click **Delete Logs Now** to delete the local logs, including all non-active log files, immediately. See [Deleting Local Log Data, page 18-27](#) for more information on deleting log data.

**Step 3** Click **Submit** to save your changes.

Your configuration is saved and the Local Configuration page is refreshed.

---

## Deleting Local Log Data

Use the Local Configuration page to manually delete your local log data. You can use this option to free up space when the local store is full. See [Local Store Target, page A-5](#) for more information about the local store.

---

**Step 1** Select **System Administration > Configuration > Log Configuration > Local Log Target**.

The Local Configuration page appears.

**Step 2** Click **Delete Logs Now** to immediately delete all local log data files, except the log data in the currently active log data file.

The Local Configuration page is refreshed.

---

# Configuring Logging Categories

This section contains the following topics:

- [Configuring Global Logging Categories, page 18-28](#)
- [Configuring Per-Instance Logging Categories, page 18-33](#)

All configuration performed for a parent logging category affects the children within the logging category. You can select a child of a parent logging category to configure it separately, and it does not affect the parent logging category or the other children.

## Configuring Global Logging Categories

To view and configure global logging categories:

- Step 1

Select **System Administration > Configuration > Log Configuration > Logging Categories > Global**.
- The Logging Categories page appears; from here, you can view the logging categories.
- Step 2

Click the name of the logging category you want to configure; or, click the radio button the name of the logging category you want to configure and click **Edit**.
- Step 3

Complete the fields as described in [Table 18-22](#).

Table 18-22 Global: General Page

| Option                                      | Descriptions                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Configure Log Category</b>               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Log Severity                                | For diagnostic logging categories, use the drop-down list box to select the severity level. (For audit and accounting categories, there is only one severity, NOTICE, which cannot be modified.) Valid options are: <ul style="list-style-type: none"> <li>• FATAL—Emergency. ACS is not usable and you must take action immediately.</li> <li>• ERROR—Critical or error condition.</li> <li>• WARN—Normal, but significant condition. (Default)</li> <li>• INFO—Informational message.</li> <li>• DEBUG—Diagnostic bug message.</li> </ul> |
| <b>Configure Local Setting for Category</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Log to Local Target                         | Check to enable logging to the local target.<br><br>For administrative and operational audit logging category types, logging to local target is enabled by default and cannot be disabled.                                                                                                                                                                                                                                                                                                                                                  |
| Local Target is Critical                    | <i>Usable for accounting and for AAA audit (passed authentication) logging category types only.</i> Check the check box to make this local target the critical target.<br><br>For administrative and operational audit logging category types, the check box is checked by default and cannot be unchecked; the local target is the critical target.                                                                                                                                                                                        |
| <b>Configure Logged Attributes</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| —                                           | <i>Display only.</i> All attributes are logged to the local target.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |



If you have completed your configuration, proceed to [Step 6](#).

**Step 4** To configure a remote syslog target, click the **Remote Syslog Target** and proceed to [Step 5](#).

**Step 5** Complete the Remote Syslog Target fields as described in [Table 18-23](#):

**Table 18-23** Global: Remote Syslog Target Page

| Option                          | Description                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Configure Syslog Targets</b> |                                                                                                                                                  |
| Available targets               | List of available targets. You can select a target from this list and move it to the Selected Targets list.                                      |
| Selected targets                | List of selected targets. You can select a target from this list and move it to the Available Targets list to remove it from your configuration. |

**Step 6** Click **Submit**.

The Logging Categories page appears, with your configured logging category.

Administrative and operational audit messages include audit messages of the following types:

- Configuration changes
- Internal user change password
- Administrator access
- Operational audit

Some of the operational audit messages are not logged in the local log target. See [Table 18-24](#) for a list of administrative and operational logs that are not logged in the local target. See [Viewing ADE-OS Logs, page 18-32](#) for information on how you can view these logs from the ACS CLI.

[Table 18-24](#) lists a set of administrative and operational logs under various categories that are not logged to the local target.

**Table 18-24** *Administrative and Operational Logs Not Logged in the Local Target*

| Category           | Log and Description                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Process-Management | <ul style="list-style-type: none"> <li>• ACS_START_PROCESS—ACS process started</li> <li>• ACS_STOP_PROCESS—ACS process stopped</li> <li>• ACS_START—All ACS processes started</li> <li>• ACS_STOP—All ACS processes stopped</li> <li>• WD_RESTART_PROCESS—ACS process restarted by watchdog</li> <li>• WD_CONFIG_CHANGE—Watchdog configuration reloaded</li> <li>• ACS_START_STOP_ERROR—ACS process reported start/stop error</li> </ul> |
| DB-Management      | <ul style="list-style-type: none"> <li>• CARS_BACKUP—CARS backup complete</li> <li>• CARS_RESTORE—CARS restore complete</li> <li>• ACS_BACKUP—ACS DB backup complete</li> <li>• ACS_RESTORE—ACS DB restore complete</li> <li>• ACS_SUPPORT—ACS support bundle collected</li> <li>• ACS_RESET—ACS DB reset</li> </ul>                                                                                                                     |
| File-Management    | <ul style="list-style-type: none"> <li>• ACS_DELETE_CORE—ACS core files deleted</li> <li>• ACS_DELETE_LOG—ACS log files deleted</li> </ul>                                                                                                                                                                                                                                                                                               |

Table 18-24 Administrative and Operational Logs Not Logged in the Local Target (continued)

| Category            | Log and Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Software-Management | <ul style="list-style-type: none"> <li>• ACS_UPGRADE—ACS upgraded</li> <li>• ACS_PATCH—ACS patch installed</li> <li>• UPGRADE_SCHEMA_CHANGE—ACS schema upgrade complete</li> <li>• UPGRADE_DICTIONARY—ACS dictionary upgrade complete</li> <li>• UPGRADE_DATA_MANIPULATION—ACS upgrade - data manipulation stage complete</li> <li>• UPGRADE_AAC—ACS AAC upgrade complete</li> <li>• UPGRADE_PKI—ACS PKI upgrade complete</li> <li>• UPGRADE_VIEW—ACS View upgrade complete</li> <li>• CLI_ACS_UPGRADE—ACS upgrade started</li> <li>• CLI_ACS_INSTALL—ACS install started</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| System-Management   | <ul style="list-style-type: none"> <li>• ACS_MIGRATION_INTERFACE—ACS migration interface enabled/disabled</li> <li>• ACS_ADMIN_PSWD_RESET—ACS administrator password reset</li> <li>• CLI_CLOCK_SET—Clock set</li> <li>• CLI_TZ_SET—Time zone set</li> <li>• CLI_NTP_SET—NTP Server set</li> <li>• CLI_HOSTNAME_SET—Hostname set</li> <li>• CLI_IPADDRESS_SET—IP address set</li> <li>• CLI_IPADDRESS_STATE—IP address state</li> <li>• CLI_DEFAULT_GATEWAY—Default gateway set</li> <li>• CLI_NAME_SERVER—Name server set</li> <li>• ADEOS_XFER_LIBERROR—ADE OS Xfer library error</li> <li>• ADEOS_INSTALL_LIBERROR—ADE OS install library error</li> <li>• AD_JOIN_ERROR—AD agent failed to join AD domain</li> <li>• AD_JOIN_DOMAIN—AD agent joined AD domain</li> <li>• AD_LEAVE_DOMAIN—AD agent left AD domain</li> <li>• IMPORT_EXPORT_PROCESS_ABORTED—Import/Export process aborted</li> <li>• IMPORT_EXPORT_PROCESS_STARTED—Import/Export process started</li> <li>• IMPORT_EXPORT_PROCESS_COMPLETED—Import/Export process completed</li> <li>• IMPORT_EXPORT_PROCESS_ERROR—Error while Import/Export process</li> </ul> |

**Related Topic**

- [Configuring Per-Instance Logging Categories, page 18-33](#)
- [Viewing ADE-OS Logs, page 18-32](#)

## Viewing ADE-OS Logs

The logs listed in [Table 18-24](#) are written to the ADE-OS logs. From the ACS CLI, you can use the following command to view the ADE-OS logs:

### **show logging system ade/ADE.log**

This command lists all the ADE-OS logs and your output would be similar to the following example.

```
Sep 29 23:24:15 cd-ac5-13-179 sshd(pam_unix)[20013]: 1 more authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95
user=admin
Sep 29 23:24:34 cd-ac5-13-179 sshd(pam_unix)[20017]: authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95 user=admin
min
Sep 29 23:24:36 cd-ac5-13-179 sshd[20017]: Failed password for admin from 10.77.137.95
port 3635 ssh2
Sep 30 00:47:44 cd-ac5-13-179 sshd(pam_unix)[20946]: authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95 user=admin
min
Sep 30 00:47:46 cd-ac5-13-179 sshd[20946]: Failed password for admin from 10.77.137.95
port 3953 ssh2
Sep 30 00:54:59 cd-ac5-13-179 sshd(pam_unix)[21028]: authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=10.77.137.95 user=admin
min
Sep 30 00:55:01 cd-ac5-13-179 sshd[21028]: Failed password for admin from 10.77.137.95
port 3962 ssh2
Sep 30 00:55:35 cd-ac5-13-179 last message repeated 5 times
Sep 30 00:55:39 cd-ac5-13-179 sshd[21028]: Accepted password for admin from 10.77.137.95
port 3962 ssh2
Sep 30 00:55:39 cd-ac5-13-179 sshd(pam_unix)[21038]: session opened for user admin by
(uid=0)
Sep 30 00:55:40 cd-ac5-13-179 debugd[2597]: hangup signal caught, configuration read
Sep 30 00:55:40 cd-ac5-13-179 debugd[2597]: successfully loaded debug config
Sep 30 00:55:40 cd-ac5-13-179 debugd[2597]: [21043]: utils: cars_shellcfg.c[118] [admin]:
Invoked carsGetConsoleConfig
Sep 30 00:55:40 cd-ac5-13-179 debugd[2597]: [21043]: utils: cars_shellcfg.c[135] [admin]:
No Config file, returning defaults
Sep 30 01:22:20 cd-ac5-13-179 sshd[21038]: Received disconnect from 10.77.137.95: 11:
Connection discarded by broker
Sep 30 01:22:20 cd-ac5-13-179 sshd(pam_unix)[21038]: session closed for user admin
Sep 30 01:22:22 cd-ac5-13-179 debugd[2597]: hangup signal caught, configuration read
Sep 30 01:22:22 cd-ac5-13-179 debugd[2597]: successfully loaded debug config
Sep 30 02:48:54 cd-ac5-13-179 sshd[22500]: Accepted password for admin from 10.77.137.58
port 4527 ssh2
Sep 30 02:48:54 cd-ac5-13-179 sshd(pam_unix)[22504]: session opened for user admin by
(uid=0)
Sep 30 02:48:55 cd-ac5-13-179 debugd[2597]: hangup signal caught, configuration read
Sep 30 02:48:55 cd-ac5-13-179 debugd[2597]: successfully loaded debug config
```

You can view the logs grouped by the module that they belong to. For example, the monitoring and troubleshooting logs contain the string **MSGCAT** and the debug logs contain the string **debug**.

From the ACS CLI, you can enter the following two commands to view the monitoring and troubleshooting logs and the administrative logs respectively:

- **show logging system | include MSGCAT**
- **show logging system | include debug**

The output of the **show logging system | include MSGCAT** would be similar to:

```
Sep 27 13:00:02 cd-ac5-13-103 MSGCAT58010/root: info:[ACS backup] ACS backup completed
Sep 28 13:00:03 cd-ac5-13-103 MSGCAT58010/root: info:[ACS backup] ACS backup completed
Sep 29 06:28:17 cd-ac5-13-103 MSGCAT58007: Killing Tomcat 8363
```

```

Sep 29 06:28:28 cd-accs5-13-103 MSGCAT58004/admin: ACS Stopped
Sep 29 06:31:41 cd-accs5-13-103 MSGCAT58037/admin: Installing ACS
Sep 29 09:52:35 cd-accs5-13-103 MSGCAT58007: Killing Tomcat 32729
Sep 29 09:52:46 cd-accs5-13-103 MSGCAT58004/admin: ACS Stopped
Sep 29 09:53:29 cd-accs5-13-103 MSGCAT58004/admin: ACS Starting
Sep 29 10:37:45 cd-accs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration enable
Sep 29 13:00:02 cd-accs5-13-103 MSGCAT58010/root: info:[ACS backup] ACS backup completed
Sep 29 13:56:36 cd-accs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration disable
Sep 29 13:57:02 cd-accs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration disable
Sep 29 13:57:25 cd-accs5-13-103 MSGCAT58018/admin: [ACS-modify-migration-state] completed
successfully - interface migration enable
Sep 30 10:57:10 cd-accs5-13-103 MSGCAT58010/admin: info:[ACS backup] ACS backup completed

```

For more information on the **show logging** command, refer to [CLI Reference Guide for Cisco Secure Access Control System 5.8.1](#).

## Configuring Per-Instance Logging Categories

You can define a custom logging category configuration for specific, overridden ACS instances, or return all instances to the default global logging category configuration.

To view and configure per-instance logging categories:

- 
- Step 1** Select **System Administration > Configuration > Log Configuration > Logging Categories > Per-Instance**.

The Per-Instance page appears; from here, you can view the individual ACS instances of your deployment.

- Step 2** Click the radio button associated with the name of the ACS instance you want to configure, and choose one of these options:
- Click **Override** to override the current logging category configuration for selected ACS instances.
  - Click **Configure** to display the Logging Categories page associated with the ACS instance. You can then edit the logging categories for the ACS instance. See [Displaying Logging Categories, page 18-35](#) for field descriptions.
  - Click **Restore to Global** to restore selected ACS instances to the default global logging category configuration.

Your configuration is saved and the Per-Instance page is refreshed.

---

### Related Topic

- [Configuring Per-Instance Security and Log Settings, page 18-33](#)

## Configuring Per-Instance Security and Log Settings

You can configure the severity level and local log settings in a logging category configuration for a specific overridden or custom ACS instance. Use this page to:

- View a tree of configured logging categories for a specific ACS instance.

- Open a page to configure a logging category's severity level, log target, and logged attributes for a specific ACS instance.

**Step 1** Select **System Administration > Configuration > Log Configuration > Logging Categories > Per-Instance**, then click **Configure**.

The Per-Instance: Configuration page appears as described in [Table 18-25 on page 34](#):

**Table 18-25** *Per-Instance: Configuration Page*

| Option | Description                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Name   | Expandable tree structure of AAA service logging categories.                                                                              |
| Edit   | Click to display a selected Logging Categories > Edit: " <i>lc_name</i> " page, where <i>lc_name</i> is the name of the logging category. |

**Step 2** Do one of the following:

- Click the name of the logging category you want to configure.
- Select the radio button associated with the name of the logging category you want to configure, and click **Edit**.

The Per-Instance: General page appears.

From here, you can configure the security level and local log settings in a logging category configuration for a specific ACS instance. See [Table 18-26](#):

**Table 18-26** *Per-Instance: General Page*

| Option                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Configure Log Category</b>               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Log Severity                                | Use the list box to select the severity level for diagnostic logging categories. (For audit and accounting categories, there is only one severity, NOTICE, which cannot be modified.) Valid options are: <ul style="list-style-type: none"> <li>• FATAL—Emergency. The ACS is not usable and you must take action immediately.</li> <li>• ERROR—Critical or error condition.</li> <li>• WARN—Normal, but significant condition. (Default)</li> <li>• INFO—Informational message.</li> <li>• DEBUG—Diagnostic bug message.</li> </ul> |
| <b>Configure Local Setting for Category</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Log to Local Target                         | Check to enable logging to the local target.<br><br>For administrative and operational audit logging category types, logging to local target is enabled by default and cannot be disabled.                                                                                                                                                                                                                                                                                                                                           |
| Local Target is Critical                    | <i>Usable for accounting and for passed authentication logging category types only.</i> Check the check box to make this local target the critical target.<br><br>For administrative and operational audit logging category types, the check box is checked by default and cannot be unchecked; the local target is the critical target.                                                                                                                                                                                             |
| <b>Configure Logged Attributes</b>          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| —                                           | <i>Display only.</i> All attributes are logged to the local target.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Configuring Per-Instance Remote Syslog Targets

Use this page to configure remote syslog targets for logging categories.

- Step 1** Select **System Administration > Configuration > Log Configuration > Logging Categories > Per-Instance**, then click **Configure**.
- The Per-Instance: Configuration page appears as described in [Table 18-25](#).
- Step 2** Do one of the following actions:
- Click the name of the logging category you want to configure.
  - Select the radio button associated with the name of the logging category you want to configure, and click **Edit**.
- Step 3** Click the **Remote Syslog Target** tab.
- The Per-Instance: Remote Syslog Targets page appears as described in [Table 18-27](#):

**Table 18-27** Per-Instance: Remote Syslog Targets Page

| Option                          | Description                                                                                                                                      |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Configure Syslog Targets</b> |                                                                                                                                                  |
| Available targets               | List of available targets. You can select a target from this list and move it to the Selected Targets list.                                      |
| Selected targets                | List of selected targets. You can select a target from this list and move it to the Available Targets list to remove it from your configuration. |

## Displaying Logging Categories

You can view a tree of configured logging categories for a specific ACS instance. In addition, you can configure a logging category's severity level, log target, and logged attributes for a specific ACS instance.

- Step 1** Select **System Administration > Configuration > Log Configuration > Logging Categories > Per-Instance**, then click **Configure**.
- Step 2** Complete the fields as described in [Table 18-28](#):

**Table 18-28** Per-Instance: Configuration Page

| Option | Description                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Name   | Expandable tree structure of AAA services logging categories.                                                                             |
| Edit   | Click to display a selected Logging Categories > Edit: " <i>lc_name</i> " page, where <i>lc_name</i> is the name of the logging category. |

## Configuring the Log Collector

Use the Log Collector page to select a log data collector and suspend or resume log data transmission.

**Step 1** Select **System Administration > Configuration > Log Configuration > Log Collector**.

The Log Collector page appears.

**Step 2** Complete the Log Collector fields as described in [Table 18-29](#):

**Table 18-29** *Log Collector Page*

| Option                    | Description                                                                                                  |
|---------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Log Data Collector</b> |                                                                                                              |
| Current Log Collector     | <i>Display only.</i> Identifies the machine on which the local log messages are sent.                        |
| Select Log Collector      | Use the drop-down list box to select the machine on which you want local log messages sent.                  |
| Set Log Collector         | Click to configure the log collector according to the selection you make in the Select Log Collector option. |

**Step 3** Do one of the following:

- Click **Suspend** to suspend the log data transmission to the configured log collector.
- Click **Resume** to resume the log data transmission to the configured log collector.

Your configuration is saved and the Log Collector page is refreshed.

## Viewing the Log Message Catalog

Use the Log Message Catalog page to view all possible log messages.

Choose **System Administration > Configuration > Log Configuration > Log Message Catalog**.

The Log Message Catalog page appears, with the fields described in [Table 18-30](#), from which you can view all possible log messages that can appear in your log files.

**Table 18-30** *Log Messages Page*

| Option        | Description                                                                                 |
|---------------|---------------------------------------------------------------------------------------------|
| Message Code  | <i>Display only.</i> A unique message code identification number associated with a message. |
| Severity      | <i>Display only.</i> The severity level associated with a message.                          |
| Category      | <i>Display only.</i> The logging category to which a message belongs.                       |
| Message Class | <i>Display only.</i> The group to which a message belongs.                                  |
| Message Text  | <i>Display only.</i> English language message text (name of the message).                   |
| Description   | <i>Display only.</i> English language text that describes the associated message.           |



## Exporting Messages from the Log Message Catalog

ACS 5.8.1 provides the option to download syslog messages with message codes and description in the form of a CSV file. When you export the syslog messages, the filtering option does not work. ACS exports all syslog messages that are available in the Log Message Catalog page. The progress bar is not displayed during the export operation. If the export operation fails, ACS does not prompt to save the .csv file or the file can be empty.

Use the Log Message Catalog page to export log messages.

- 
- Step 1** Choose **System Administration > Configuration > Log Configuration > Log Message Catalog**.  
The Log Message Catalog page appears, with the fields described in [Table 18-30](#), from which you can view all possible log messages that can appear in your log files.
- Step 2** Click **Export**.  
ACS exports all syslog messages that are available in the Log Message Catalog page as a .csv file.
- Step 3** Specify a location and click **Save**.  
The .csv file is saved in the specified location.
- 

## Licensing Overview

To operate ACS, you must install a valid license. ACS prompts you to install a valid base license when you first access the web interface. Each ACS instance (primary or secondary) in a distributed deployment requires a unique base license.

**Note**

---

Each server requires a unique base license in a distributed deployment.

---

## Types of Licenses

Table 18-31 shows the ACS 5.8.1 license support:

**Table 18-31** *ACS License Support*

| License                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Base License                  | <p>Required for all software instances deployed, as well as for all appliances. The base license enables you to use all the ACS functionality except license controlled features, and it enables all reporting features. Base license is:</p> <ul style="list-style-type: none"> <li>• Required for each ACS instance, primary and secondary.</li> <li>• Required for all appliances.</li> <li>• Supports deployments with up to 500 network devices (AAA clients).</li> </ul> <p>Base licenses are of two types:</p> <ul style="list-style-type: none"> <li>• Permanent—Supports up to 500 network devices (AAA clients).</li> <li>• Eval—Supports up to 50 network devices and expires in 90 days.</li> </ul> <p>The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256.</p> <p>If your evaluation license expires or is about to expire, you cannot use another evaluation license or extend your current license. Before your evaluation license expires, you must upgrade to a Permanent license.</p> |
| Add-on Licenses               | <p>Supports an unlimited number of managed devices. Requires an existing ACS permanent base license. There are also evaluation-type licenses for add-on licenses.</p> <p>The Security Group Access feature licenses are of three types: Permanent, Eval, and NFR. However, the permanent Security Group Access feature license can be used only with a permanent base license.</p> <p>Also, the large deployment license can only be used only with a permanent base license.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Evaluation License (standard) | <p>Enables standard centralized reporting features.</p> <ul style="list-style-type: none"> <li>• Cannot be reused on the same platform.</li> <li>• You can only install one evaluation license per platform. You cannot install additional evaluation licenses.</li> <li>• Supports 50 managed devices.</li> <li>• Expires 90 days from the time the license is installed.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

### Related Topics

- [Licensing Overview, page 18-37](#)
- [Installing a License File, page 18-39](#)
- [Viewing and Upgrading the Base Server License, page 18-39](#)
- [Adding Deployment License Files, page 18-42](#)
- [Deleting Deployment License Files, page 18-43](#)

# Installing a License File

You can obtain a valid license file using the Product Activation Key (PAK) supplied with the product. To install a license file:

- 
- Step 1** Log into the ACS web interface.
- The Initial Licenses page appears when you log in to the ACS machine for the first time.
- Step 2** Click **Cisco Secure ACS License Registration**.
- This link directs you to Cisco.com to purchase a valid license file from a Cisco representative.
- Step 3** Click **Install** to install the license file that you purchased.
- The ACS web interface log in page reappears. You can now work with the ACS application.
- 

## Related Topics

- [Licensing Overview, page 18-37](#)
- [Viewing and Upgrading the Base Server License, page 18-39](#)
- [Adding Deployment License Files, page 18-42](#)
- [Deleting Deployment License Files, page 18-43](#)

## Viewing and Upgrading the Base Server License

ACS 5.8.1 allows you to upgrade or modify a base license without performing the reset config operation. To view and upgrade the base license:

- 
- Step 1** Select **System Administration > Configuration > Licensing > Base Server License**.
- The Base Server License page appears with a description of the ACS deployment configuration and a list of the available deployment licenses. See [Types of Licenses, page 18-38](#) for a list of deployment licenses.
- [Table 18-32](#) describes the fields in the Base Server License page.

**Table 18-32**      *Base Server License Page*

| Option                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ACS Deployment Configuration</b>                          |                                                                                                                                                                                                                                                                                                                                                                                                  |
| Primary ACS Instance                                         | Name of the primary instance created when you logged into the ACS 5.8.1 web interface.                                                                                                                                                                                                                                                                                                           |
| Number of Instances                                          | Current number of ACS instances (primary or secondary) in the ACS database.                                                                                                                                                                                                                                                                                                                      |
| Current Number of Configured IP Addresses in Network Devices | Total number of IP addresses in all the subnetworks that you have configured as part of network device configuration.<br><br>The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256. |

Table 18-32 Base Server License Page (continued)

| Option                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum Number of IP Addresses in Network Devices | <p>Maximum number of IP addresses that your license supports:</p> <ul style="list-style-type: none"> <li>Base License—Supports 500 IP addresses.</li> </ul> <p>The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256.</p> <ul style="list-style-type: none"> <li>Large Deployment—Supports an unlimited number of IP addresses.</li> </ul> |
| Use this link to obtain a valid License File      | Directs you to Cisco.com to generate a valid license file using the Product Activation Key (PAK)                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Base License Configuration</b>                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| ACS Instance                                      | Name of the ACS instance, either primary or secondary.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Identifier                                        | Name of the base license.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| License Type                                      | Specifies the base license type (permanent, evaluation).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Expiration                                        | Specifies the expiration date for evaluation licenses. For permanent licenses, the expiration field indicates <i>permanent</i> .                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Licensed to                                       | Name of the company that this product is licensed to.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| PAK                                               | Name of the Product Activation Key (PAK) received from Cisco.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Version                                           | Current version of the ACS software.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Step 2** Select the radio button the instance whose license you want to upgrade and click **Upgrade/Modify**.

The Base Server License Edit page appears.

The administrator can upgrade or modify a base license from ACS 5.8.1 web interface without resetting the configuration.

**Step 3** Complete the fields as described in [Table 18-33](#):

Table 18-33 Base Server License Edit Page

| Option                                       | Description                                                                                    |
|----------------------------------------------|------------------------------------------------------------------------------------------------|
| <b>ACS Instance License Configuration</b>    |                                                                                                |
| Version                                      | Displays the current version of the ACS software.                                              |
| ACS Instance                                 | Displays the name of the ACS instance, either primary or secondary.                            |
| License Type                                 | Specifies the license type.                                                                    |
| Use this link to obtain a valid License File | Directs you to Cisco.com to purchase a valid license file from a Cisco representative.         |
| <b>License Location</b>                      |                                                                                                |
| License File                                 | Click <b>Browse</b> to navigate to the directory that contains the license file and select it. |

**Step 4** Click **Submit**.

**Related Topics**

- [Licensing Overview, page 18-37](#)
- [Types of Licenses, page 18-38](#)
- [Installing a License File, page 18-39](#)
- [Adding Deployment License Files, page 18-42](#)
- [Deleting Deployment License Files, page 18-43](#)

## Viewing License Feature Options

You can add, upgrade, or delete existing deployment licenses. The configuration pane at the top of the page shows the deployment information.

Select **System Administration > Configuration > Licensing > Feature Options**.

The Feature Options Page appears as described in [Table 18-34](#):

**Table 18-34**      *Feature Options Page*

| Option                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ACS Deployment Configuration</b>                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Primary ACS Instance                                         | Name of the primary instance created when you login into the ACS 5.8.1 web interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Number of Instances                                          | Current number of ACS instances (primary or secondary) in the ACS database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Current Number of Configured IP Addresses in Network Devices | <p>Total number of IP addresses in all the subnetworks that you have configured as part of network device configuration.</p> <p>The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256.</p>                                                                                                                                                     |
| Maximum Number of IP Addresses in Network Devices            | <p>Maximum number of IP addresses that your license supports:</p> <ul style="list-style-type: none"> <li>• Base License—Supports 500 IP addresses.</li> </ul> <p>The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256.</p> <ul style="list-style-type: none"> <li>• Large Deployment—Supports an unlimited number of IP addresses.</li> </ul> |
| Use this link to obtain a valid License File                 | Directs you to Cisco.com to purchase a valid license file from a Cisco representative.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Installed Deployment License Options</b>                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Feature                                                      | <ul style="list-style-type: none"> <li>• Large Deployment—Supports an unlimited number of managed devices.</li> <li>• Security Group Access Control—Enables Cisco Trusted Server (SGA) management functionality. This requires an existing ACS base license.</li> </ul>                                                                                                                                                                                                                                                                                     |
| Licensed to                                                  | Name of the company that this product is licensed to.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| License Type                                                 | Specifies the license type (permanent, evaluation).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Expiration                                                   | <p>Expiration date for the following features:</p> <ul style="list-style-type: none"> <li>• Large Deployment</li> <li>• SGA</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                      |

Table 18-34 Feature Options Page (continued)

| Option      | Description                                                                                                                |
|-------------|----------------------------------------------------------------------------------------------------------------------------|
| Add/Upgrade | Click <b>Add/Upgrade</b> to access the <a href="#">Viewing License Feature Options, page 18-41</a> and add a license file. |
| Delete      | Select the radio button the license feature you wish to delete and click <b>Delete</b> .                                   |

## Adding Deployment License Files

To add a new base deployment license file:

- 
- Step 1** Select **System Administration > Configuration > Licensing > Feature Options**.
- The Feature Options page appears with a description of the ACS deployment configuration and a list of the available deployment licenses and their configurations. See Add-on Licenses in [Types of Licenses, page 18-38](#) for a list of deployment licenses. See [Viewing License Feature Options, page 18-41](#) for field descriptions.
- Step 2** Click **Add**.
- The Feature Options Create page appears.
- Step 3** Complete the fields as described in [Table 18-35](#) to add a license:

Table 18-35 Feature Options Create Page

| Option                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ACS Deployment Configuration</b>                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Primary ACS Instance                                         | Name of the primary instance created when you login into the ACS 5.8.1 web interface.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Number of Instances                                          | Current number of ACS instances (primary or secondary) in the ACS database.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Current Number of Configured IP Addresses in Network Devices | Total number of IP addresses in all the subnetworks that you have configured as part of network device configuration.<br><br>The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256.                                                                                                          |
| Maximum Number of IP Addresses in Network Devices            | Maximum number of IP addresses that your license supports: <ul style="list-style-type: none"> <li>Base License—Supports 500 IP addresses.<br/><br/>The number of devices is determined by the number of unique IP addresses that you configure. This includes the subnet masks that you configure. For example, a subnet mask of 255.255.255.0 implies 256 unique IP addresses and hence the number of devices is 256.</li> <li>Large Deployment—Supports an unlimited number of IP addresses.</li> </ul> |
| Use this link to obtain a valid License File                 | Directs you to Cisco.com to purchase a valid license file from a Cisco representative.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>License Location</b>                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| License File                                                 | Click <b>Browse</b> to browse to the location of the purchased license file you wish to install and select it.                                                                                                                                                                                                                                                                                                                                                                                            |

- Step 4** Click **Submit** to download the license file.  
The Feature Options page appears with the additional license.
- 

**Related Topics**

- [Licensing Overview, page 18-37](#)
- [Types of Licenses, page 18-38](#)
- [Installing a License File, page 18-39](#)
- [Viewing and Upgrading the Base Server License, page 18-39](#)
- [Deleting Deployment License Files, page 18-43](#)

## Deleting Deployment License Files

To delete deployment license files:

- 
- Step 1** Select **System Administration > Configuration > Licensing > Feature Options**.  
The Feature Options page appears with a description of the ACS deployment configuration and a list of the available deployment licenses and their configurations. See Add-on Licenses in [Types of Licenses, page 18-38](#) for a list of deployment licenses. See the [Table 18-34](#) for field descriptions.
- Step 2** Select the radio button the deployment you wish to delete.
- Step 3** Click **Delete** to delete the license file.
- 

**Related Topics**

- [Licensing Overview, page 18-37](#)
- [Types of Licenses, page 18-38](#)
- [Installing a License File, page 18-39](#)
- [Viewing and Upgrading the Base Server License, page 18-39](#)
- [Adding Deployment License Files, page 18-42](#)

## Available Downloads

This section contains information about the utilities and files that are available for download from the ACS web interface:

- [Downloading Migration Utility Files, page 18-44](#)
- [Downloading UCP Web Service Files, page 18-44](#)
- [Downloading Sample Python Scripts, page 18-44](#)
- [Downloading Rest Services, page 18-45](#)

## Downloading Migration Utility Files

To download migration application files and the migration guide for ACS 5.8.1:

- 
- Step 1** Choose **System Administration > Downloads > Migration Utility**.  
The Migration from 4.x page appears.
- Step 2** Click **Migration application files**, to download the application file you want to use to run the migration utility.
- Step 3** Click **Migration Guide**, to download *Migration Guide for Cisco Secure Access Control System 5.8.1*.
- 

## Downloading UCP Web Service Files

You can download the WSDL file from this page to integrate ACS with your in-house portals and allow ACS users configured in the ACS internal identity store to change their own passwords. The UCP web service allows only the users to change their passwords. They can do so on the primary or secondary ACS servers.

The UCP web service compares the new password that you provide with the password policy that is configured in ACS for users. If the new password conforms to the defined criteria, your new password takes effect. After your password is changed on the primary ACS server, ACS replicates it to all the secondary ACS servers.

To download the UCP WSDL Files:

- 
- Step 1** Choose **System Administration > Downloads > User Change Password**.  
The User Change Password (UCP) web service page appears.
- Step 2** Click one of the following:
- **UCP WSDL** to download the WSDL file.
  - **UCP Web application example** to download the application file.
  - **Python Script for Using the User Change Password Web Service** to download a sample Python script.

For more information on how to use the UCP web service, refer to [Software Developer's Guide for Cisco Secure Access Control System](#).

---

## Downloading Sample Python Scripts

The Scripts page contains sample Python scripts for:

- Using the UCP web service.
- Automating the bulk import and export operations.

To download these sample scripts:



- 
- Step 1** Choose **System Administration > Downloads > Sample Python Scripts**.  
The Sample Python Scripts page appears.
- Step 2** Click one of the following:
- **Python Script for Using the User Change Password Web Service**—To download the sample script for the UCP web service.
  - **Python Script for Performing CRUD Operations on ACS Objects**—To download the sample script for the import and export process.
- Step 3** Save the script to your local hard drive.  
The scripts come with installation instructions. For more information on how to use the scripts, refer to [Software Developer's Guide for Cisco Secure Access Control System](#).
- 

**Note**

The Cisco Technical Assistance Center (TAC) supports only the default Python Script. TAC does not offer any support for modified scripts.

---

## Downloading Rest Services

ACS Rest Service allows to create, update, delete and retrieve objects from ACS Database.

**Note**

You must enable the Rest Service using the command line for reading the WADL files.

---

To download ACS Rest Service WADL files:

---

- Step 1** Choose **System Administration > Downloads > Rest Service**.  
The Rest Service Page appears.
- Step 2** Click one of the following:
- **Common or Identity**—To download XSD files that describe the structure of the objects supported on ACS 5.8.1 Rest interfaces.
  - **Schema files**—To download the Schema files.
  - **SDK Samples**—To download the SDK Samples.

**Note**

After installing ACS 5.8 patch 4 or later, ACS uses TLSv1.2 as the default SSL context. The REST SDK uses SSL as the default context until ACS 5.8 patch 6. From ACS 5.8 patch 7, the REST SDK uses TLSv1.2 as the default SSL context with the condition that the REST client should be running JRE 1.7 or later. If you want the REST SDK to use TLSv1.0/SSL, you must check the **Enable TLS 1.0 for https access** check box in the Security Settings page and then modify the SSL Context parameter as TLSv1.0/SSL in the downloaded SDK sample regardless of the REST client's JRE version.

---

For more information on how to use the Rest Services, refer to [Software Developer's Guide for Cisco Secure Access Control System](#).

---



## Understanding Logging

---

This chapter describes logging functionality in ACS 5.8.1. Administrators and users use the various management interfaces of ACS to perform different tasks. Using the administrative access control feature, you can assign permissions to administrators and users to perform different tasks.

Apart from this, you also need an option to track the various actions performed by the administrators and users. ACS offers you several logs that you can use to track these actions and events.

This chapter contains the following sections:

- [About Logging, page A-1](#)
- [ACS 4.x Versus ACS 5.8.1 Logging, page A-11](#)

## About Logging

You can gather the following logs in ACS:

- **Customer Logs**—For auditing and troubleshooting your ACS, including logs that record daily operations, such as accounting, auditing, and system-level diagnostics.
- **Debug logs**—Low-level text messages that you can export to Cisco technical support for evaluation and troubleshooting. You configure ACS debug logs, using the command line interface. Specifically, you enable and configure severity levels of the ACS debug logs using the command line interface. See *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.8.1* for more information.
- **Platform logs**—Log files generated by the ACS appliance operating system.

Debug and platform logs are stored locally on each ACS server. Customer logs can be viewed centrally for all servers in a deployment.

You can use the following ACS interfaces for logging:

- **Web interface**—This is the primary logging interface. You can configure which messages to log and to where you want the messages logged.
- **Command line interface (CLI)**—Allows you to display and download logs, debug logs, and debug backup logs to the local target. The CLI also allows you to display and download platform logs. See *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.8.1* for more information.

## Using Log Targets

You can specify to send customer log information to multiple consumers or *Log Targets* and specify whether the log messages are stored locally in text format or forwarded to syslog servers. By default, a single predefined local Log Target called *Local Store* stores data in text format on an ACS server and contains log messages from the local ACS server only. You can view records stored in the Local Store from the CLI.

In addition, you can specify that logs be forwarded to a syslog server. ACS uses syslog transport to forward logs to the Monitoring and Reports component. You can also define additional syslog servers to receive ACS log messages. For each additional syslog server you specify, you must define a remote log target.

In a distributed deployment, you should designate one of the secondary ACS servers as the Monitoring and Reports server, and specify that it receive the logs from all servers in the deployment. By default, a Log Target called the *LogCollector* identifies the Monitoring and Reports server.

In cases where a distributed deployment is used, the Log Collector option on the web interface designates which server collects the log information. It is recommended that you designate a secondary server within the deployment to act as the Monitoring and Reports server.

This section contains the following topics:

- [Logging Categories, page A-2](#)
- [Log Message Severity Levels, page A-4](#)
- [Local Store Target, page A-5](#)
- [Viewing Log Messages, page A-10](#)
- [Debug Logs, page A-11](#)

## Logging Categories

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.

A logging category is a bundle of message codes which describe a function of ACS, a flow, or a use case. The categories are arranged in a hierarchical structure and used for logging configuration. Each category has:

- Name—A descriptive name
- Type—Audit, Accounting, or Diagnostics
- Attribute list—A list of attributes that may be logged with messages associated with a category, if applicable

ACS provides these preconfigured global ACS logging categories, to which you can assign log targets (see [Local Store Target, page A-5](#)):

- Administrative and Operational audit, which can include:
  - ACS configuration changes—Logs all configuration changes made to ACS. When an item is added or edited, the configuration change events also include details of the attributes that were changed and their new values. If an edit request resulted in no attributes having new values, no configuration audit record is created.

**Note**

For complex configuration items or attributes, such as policy or DACL contents, the new attribute value is reported as "New/Updated" and the audit does not contain the actual attribute value or values.

- ACS administrator access—Logs all events that occur when an administrator accesses the system until the administrator logs out. It logs whether the administrator exits ACS with an explicit request or if the session has timed out. This log also includes login attempts that fail due to account inactivity. Login failures along with failure reasons are logged.
- ACS operational changes—Logs all operations requested by administrators, including promoting an ACS from your deployment as the primary, requesting a full replication, performing software downloads, doing a backup or restore, generating and restoring PACs, and so on.
- Internal user password change—Logs all changes made to internal user passwords across all management interfaces.

In addition, the administrative and operational audit messages must be logged to the local store. You can optionally log these messages to remote logging targets (see [Local Store Target](#), page A-5).

- AAA audit, which can include RADIUS and TACACS+ successful or failed authentications, command-access passed or failed authentications, password changes, and RADIUS request responses.
- AAA diagnostics, which can include authentication, authorization, and accounting information for RADIUS and TACACS+ diagnostic requests and RADIUS attributes requests, and identity store and authentication flow information. Logging these messages is optional.
- System diagnostic, which can include system startup and system shutdown, replication failures, and logging-related diagnostic messages:
  - Administration diagnostic messages related to the CLI and web interface
  - External server-related messages
  - Local database messages
  - Local services messages
  - Certificate related messages

Logging these messages is optional.

- System statistics, which contains information on system performance and resource utilization. It includes data such as CPU and memory usage and process health and latency for handling requests.
- Accounting, which can contain TACACS+ network access session start, stop, and update messages, as well as messages that are related to command accounting. In addition, you can log these messages to the local store. Logging these messages is optional.

The log messages can be contained in the logging categories as described in this topic, or they can be contained in the logging subcategories. You can configure each logging subcategory separately, and its configuration does not affect the parent category.

In the ACS web interface, choose **System Administration > Configuration > Logging Categories > Global** to view the hierarchical structure of the logging categories and subcategories. In the web interface, choose **Monitoring and Reports > Reports > ACS Reports** to run reports based on your configured logging categories.

Each log message contains the following information:

- Event code—A unique message code.

- **Logging category**—Identifies the category to which a log message belongs.
- **Severity level**—Identifies the level of severity for diagnostics. See [Log Message Severity Levels, page A-4](#) for more information.
- **Message class**—Identifies groups of messages of similar context, for example, RADIUS, policy, or EAP-related context.
- **Message text**—Brief English language explanatory text.
- **Description**—English language text that describes log message reasons, troubleshooting information (if applicable), and external links for more information.
- **Failure reason (optional)**—Indicates whether a log message is associated with a failure reason.

Passwords are not logged, encrypted or not.

## Global and Per-Instance Logging Categories

By default, a single log category configuration applies to all servers in a deployment. For each log category, the threshold severity of messages to be logged, whether messages are to be logged to the local target, and the remote syslog targets to which the messages are to be sent to, are defined.

The log categories are organized in a hierarchical structure so that any configuration changes you make to a parent category are applied to all the child categories. However, the administrator can apply different configurations to the individual servers in a deployment.

For example, you can apply more intensive diagnostic logging on one server in the deployment. The per-instance logging category configuration displays all servers in a deployment and indicates whether they are configured to utilize the global logging configuration or have their own *custom* configuration.

To define a custom configuration for a server, you must first select the *Override* option, and then configure the specific log category definitions for that server.

You can use the Log Message Catalog to display all possible log messages that can be generated, each with its corresponding category and severity. This information can be useful when configuring the logging category definitions.

## Log Message Severity Levels

You can configure logs of a certain severity level, and higher, to be logged for a specific logging category and add this as a configuration element to further limit or expand the number of messages that you want to save, view, and export.

For example, if you configure logs of severity level WARNING to be logged for a specific logging category, log messages for that logging category of severity level WARNING and those of a higher priority levels (ERROR and FATAL) are sent to any configured locations. [Table A-1](#) describes the severity levels and their associated priority levels.

**Table A-1** Log Message Severity Levels

| ACS Severity Level | Description                                                        | Syslog Severity Level |
|--------------------|--------------------------------------------------------------------|-----------------------|
| FATAL              | Emergency. ACS is not usable and you must take action immediately. | 1 (highest)           |
| ERROR              | Critical or error conditions.                                      | 3                     |

Table A-1 Log Message Severity Levels (continued)

| ACS Severity Level | Description                                                                                                                                                                    | Syslog Severity Level |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| WARN               | Normal, but significant condition.                                                                                                                                             | 4                     |
| NOTICE             | Audit and accounting messages. Messages of severity NOTICE are always sent to the configured log targets and are not filtered, regardless of the specified severity threshold. | 5                     |
| INFO               | Diagnostic informational message.                                                                                                                                              | 6                     |
| DEBUG              | Diagnostic message.                                                                                                                                                            | 7                     |

## Local Store Target

Log messages in the local store are text files that are sent to one log file, located at */opt/CSCOacs/logs/localStore/*, regardless of which logging category they belong to. The local store can only contain log messages from the local ACS node; the local store cannot accept log messages from other ACS nodes.

You can configure which logs are sent to the local store, but you cannot configure which attributes are sent with the log messages; *all* attributes are sent with sent log messages.

Administrative and operational audit log messages are always sent to the local store, and you can also send them to remote syslog server and Monitoring and Reports server targets.

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

*time stamp sequence\_num msg\_code msg\_sev msg\_class msg\_text attr=value*

Table A-2 describes the content of the local store syslog message format.

Table A-2 Local Store and Syslog Message Format

| Field        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| timestamp    | <p>Date of the message generation, according to the local clock of the originating ACS, in the format <i>YYYY-MM-DD hh:mm:ss:xxx +/-zh:zm</i>. Possible values are:</p> <ul style="list-style-type: none"> <li><i>YYYY</i> = Numeric representation of the year.</li> <li><i>MM</i> = Numeric representation of the month. For single-digit months (1 to 9) a zero precedes the number.</li> <li><i>DD</i> = Numeric representation of the day of the month. For single-digit days (1 to 9), a zero precedes the number.</li> <li><i>hh</i> = The hour of the day—00 to 23.</li> <li><i>mm</i> = The minute of the hour—00 to 59.</li> <li><i>ss</i> = The second of the minute—00 to 59.</li> <li><i>xxx</i> = The millisecond of the second—000 to 999.</li> <li><i>+/-zz:zz</i> = The time zone offset from the ACS 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.</li> </ul> <p>For example, +02:00 indicates that the message occurred at the time indicated by the time stamp, and on an ACS node that is two hours ahead of the ACS server's time zone.</p> |
| sequence_num | Global counter of each message. If one message is sent to the local store and the the syslog server target, the counter increments by 2. Possible values are 0000000001 to 999999999.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| msg_code     | Message code as defined in the logging categories.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| msg_sev      | Message severity level of a log message (see <a href="#">Table A-1</a> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| msg_class    | Message class, which identifies groups of messages with the same context.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| text_msg     | English language descriptive text message.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| attr=value   | <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 ACS 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. For example:</p> <p>Response={RadiusPacketType=AccessAccept; AuthenticationResult=UnknownUser;<br/>cisco-av-pair=sga:security-group-tag=0000-00; }</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

You can use the web interface to configure the number of days to retain local store log files; however, the default setting is to purge data when it exceeds 5 MB or each day, whichever limit is first attained.

If you do configure more than one day to retain local store files and the data size of the combined files reaches 95000Mb, a FATAL message is sent to the system diagnostic log, and all logging to the local store is stopped until data is purged. Use the web interface to purge local store log files. Purging actions are logged to the current, active log file. See [Deleting Local Log Data, page 18-27](#).

The current log file is named *acsLocalStore.log*. Older log files are named in the format *acsLocalStore.log.YYYY-MM-DD-hh-mm-ss-xxx*, where:



- `acsLocalStore.log` = The prefix of a non-active local store log file, appended with the time stamp.



**Note** The time stamp is added when the file is first created, and should match the time stamp of the first log message in the file.

- *YYYY* = Numeric representation of the year.
- *MM* = Numeric representation of the month. For single-digit months (1 to 9), a zero precedes the number.
- *DD* = Numeric representation of the day of the month. For single-digit days (1 to 9), a zero precedes the number.
- *hh* = Hour of the day—00 to 23.
- *mm* = Minute of the hour—00 to 59.
- *ss* = Second of the minute—00 to 59.
- *xxx* = Millisecond of the second—000 to 999.

You can configure the local store to be a critical log target. See [Viewing Log Messages, page A-10](#) for more information on critical log targets.

You can send log messages to the local log target (local store) or to up to eight remote log targets (on a remote syslog server):

- Select **System Administration > Configuration > Log Configuration > Remote Log Targets** to configure remote log targets.
- Select **System Administration > Configuration > Log Configuration > Logging Categories** to configure which log messages you want to send to which targets.

## Critical Log Target

The local store target can function as a critical log target—the primary, or mandatory, log target for a logging category.

For example, administrative and operational audit messages are always logged to the local store, but you can also configure them to be logged to a remote syslog server or the Monitoring and Reports server log target. However, administrative and operational audit messages configured to be additionally logged to a remote log target are only logged to that remote log target if they are first logged successfully to the local log target.

When you configure a critical log target, and a message is sent to that critical log target, the message is also sent to the configured noncritical log target on a best-effort basis.

- When you configure a critical log target, and a message does not log to that critical log target, the message is also not sent to the configured noncritical log.
- When you do not configure a critical log target, a message is sent to a configured noncritical log target on a best-effort basis.

Select **System Administration > Configuration > Log Configuration > Logging Categories > Global > *log\_category***, where *log\_category*, is a specific logging category to configure the critical log target for the logging categories.

**Note**

Critical logging is applicable for accounting and AAA audit (passed authentications) categories only. You cannot configure critical logging for the following categories: AAA diagnostics, system diagnostics, and system statistics.

## Remote Syslog Server Target

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.

Log messages are sent to the remote syslog server with this syslog message header format, which precedes the local store syslog message format (see [Table A-2](#)):

*pri\_num YYYY Mmm DD hh:mm:ss xx:xx:xx:xx/host\_name cat\_name msg\_id total\_seg seg\_num*

Table A-3 describes the content of the remote syslog message header format.

**Table A-3 Remote Syslog Message Header Format**

| Field                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pri_num               | <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. The facility code valid options are:</p> <ul style="list-style-type: none"> <li>• LOCAL0 (Code = 16)</li> <li>• LOCAL1 (Code = 17)</li> <li>• LOCAL2 (Code = 18)</li> <li>• LOCAL3 (Code = 19)</li> <li>• LOCAL4 (Code = 20)</li> <li>• LOCAL5 (Code = 21)</li> <li>• LOCAL6 (Code = 22; default)</li> <li>• LOCAL7 (Code = 23)</li> </ul> <p>Severity value—See Table A-1 for severity values.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| time                  | <p>Date of the message generation, according to the local clock of the originating ACS, in the format <i>YYYY Mmm DD hh:mm:ss</i>. Possible values are:</p> <ul style="list-style-type: none"> <li>• <i>YYYY</i> = Numeric representation of the year.</li> <li>• <i>Mmm</i> = Representation of the month—Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec.</li> <li>• <i>DD</i> = Numeric representation of the day of the month. For single-digit days (1 to 9), a space precedes the number.</li> <li>• <i>hh</i> = The hour of the day—00 to 23.</li> <li>• <i>mm</i> = The minute of the hour—00 to 59.</li> <li>• <i>ss</i> = The second of the minute—00 to 59.</li> </ul> <p>Some device send messages that specify a time zone in the format <i>-/+hhmm</i>, where <i>-</i> and <i>+</i> identifies the directional offset from the ACS server's time zone, <i>hh</i> is the number of offset hours, and <i>mm</i> is the number of minutes of the offset hour. For example, <i>+02:00</i> indicates that the message occurred at the time indicated by the time stamp, and on an ACS node that is two hours ahead of the ACS server's time zone.</p> |
| xx:xx:xx:xx/host_name | IP address of the originating ACS, or the hostname.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| cat_name              | Logging category name preceded by the <code>CSCOacs</code> string.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| msg_id                | 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| total_seg             | Total number of segments in a log message. Long messages are divided into more than one segment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| seg_num               | 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 Message Format, which is described in Table A-2.

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.

The remote syslog server cannot function as a critical log target. See [Critical Log Target, page A-7](#) for more information on critical log targets.

## Monitoring and Reports Server Target

You can use the web interface to configure logging category messages so that they are sent to the Monitoring and Reports server target. Log messages are sent to the Monitoring and Reports server target in accordance with the syslog protocol standard (see RFC-3164). The syslog protocol is an unsecure UDP protocol.

Log messages are sent to the Monitoring and Reports server with the syslog message header format described in [Table A-3](#), which precedes the local store syslog message format (see [Table A-2](#)).

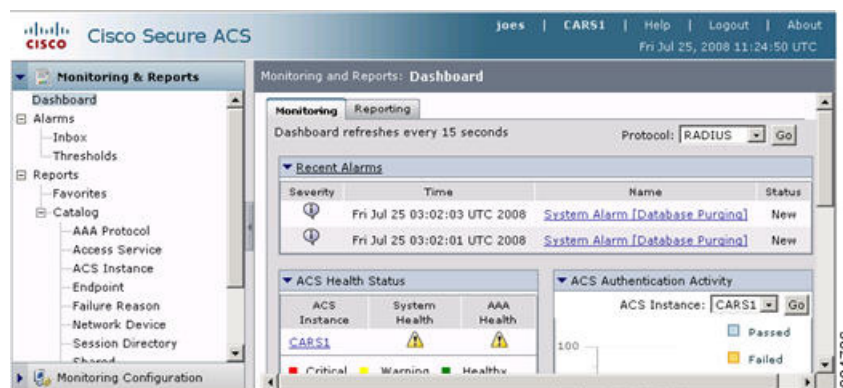
The Monitoring and Reports server cannot function as a critical log target. See [Critical Log Target, page A-7](#) for more information on critical log targets.

## Viewing Log Messages

You can use the web interface and the CLI to view locally stored log messages. You cannot view log messages that are sent to remote syslog servers via the web interface or the CLI.

In the web interface, choose **Monitoring and Reports > Launch Monitoring and Report Viewer** to open the Monitoring and Reports Viewer in a secondary window (see [Figure A-1](#)). See *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.8.1* for more information about viewing log messages via the CLI.

**Figure A-1** Monitoring and Reports Viewer



The Monitoring and Report Viewer has two drawer options:

- **Monitoring and Reports**—Use this drawer to view and configure alarms, view log reports, and perform troubleshooting tasks.
- **Monitoring Configuration**—Use this drawer to view and configure logging operations and system settings.

In addition to the information that is captured in the log messages described in [Logging Categories, page A-2](#), the Viewer reports list successful and failed AAA authentication attempts with Step attributes. Step attributes provide information about other events that occurred within the same session. This information allows you to see the sequence of steps that resulted in an authentication success or failure.

You can use the Viewer to:

- Manage alarms, reports, and troubleshooting information.
- Manage system operations, including purging data, collecting logs, scheduling jobs, and monitoring status
- Manage system configuration, including editing failure reasons, and configuring e-mail, session directory, and alarm settings

See [Monitoring and Reporting in ACS, page 11-1](#) for more information

## Debug Logs

You can use the web interface and the CLI to send logs, including debug logs, to Cisco technical support personnel if you need troubleshooting assistance. In the web interface, choose **Monitoring and Reports > Launch Monitoring and Report Viewer > Monitoring and Reports > Troubleshooting > ACS Support Bundle**.

You can also use the CLI to view and export the hardware server in the Application Deployment Engine-OS 1.2 environment logs. These messages are sent to `/var/log/boot.log` only and are unrelated to the way in which the CLI views or exports ACS debug log messages. See the *Command Line Interface Reference Guide for Cisco Secure Access Control System 5.8.1* for information.

## ACS 4.x Versus ACS 5.8.1 Logging

If you are familiar with the logging functionality in ACS 4.x, ensure that you familiarize yourself with the logging functionality of ACS 5.8.1, which is considerably different. [Table A-4](#) describes the differences between the logging functionality of ACS 4.x and ACS 5.8.1.

Table A-4 ACS 4.x vs. ACS 5.8.1 Logging Functionality

| This logging function...     | is handled this way in ACS 4.x...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | and this way in ACS 5.8.1                                                                                                                                                                                 |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Types                    | <ul style="list-style-type: none"> <li>AAA-related logs contain information about the use of remote access services by users.</li> <li>Audit logs contain information about the ACS system and activities and, therefore, record system-related events.</li> </ul> <p>These logs are useful for troubleshooting or audits. CSV audit logs are always enabled, and you can enable or disable audit logs to other loggers. You cannot configure the audit log content.</p> <p>Audit logs can display the actual changes administrators have made for each user. ACS audit logs list all the attributes that were changed for a given user.</p> | See <a href="#">Logging Categories</a> , page A-2.                                                                                                                                                        |
| Available Log Targets        | <ul style="list-style-type: none"> <li>CSV Logger</li> <li>Syslog Logger</li> <li>ODBC Logger</li> <li>Remote Logging</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | See <a href="#">Remote Syslog Server Target</a> , page A-8 and <a href="#">Local Store Target</a> , page A-5.                                                                                             |
| Log File Locations           | <ul style="list-style-type: none"> <li>CSV Logger:<br/><code>sysdrive:\Program Files\CiscoSecure ACS vx.x.</code></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <ul style="list-style-type: none"> <li>Local store target logs:<br/><code>/opt/CSCOacs/logs/localStore/</code>.</li> <li>Remote syslog server target logs:<br/><code>/var/log/messages</code>.</li> </ul> |
| Report Types                 | <ul style="list-style-type: none"> <li>CSV</li> <li>Dynamic Administration</li> <li>Entitlement</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | See <a href="#">Monitoring and Reporting in ACS</a> , page 11-1.                                                                                                                                          |
| Error Codes and Message Text | For ACS 4.2, CSAuth diagnostic logs display a description of client requests and responses. Previous versions of ACS used a numeric code for client requests and responses.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | All messages, see <a href="#">Viewing Log Messages</a> , page A-10.                                                                                                                                       |

Table A-4 ACS 4.x vs. ACS 5.8.1 Logging Functionality (continued)

| This logging function...             | is handled this way in ACS 4.x...                                                                                                                                                                                                                                        | and this way in ACS 5.8.1                                                                                                                                  |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Configuration                        | Use the <b>System Configuration &gt; Logging</b> page to define: <ul style="list-style-type: none"> <li>• Loggers and individual logs</li> <li>• Critical loggers</li> <li>• Remote logging</li> <li>• CSV log file</li> <li>• Syslog log</li> <li>• ODBC log</li> </ul> | See <a href="#">Configuring Local and Remote Log Storage, page 18-23</a> and the <i>CLI Reference Guide for Cisco Secure Access Control System 5.8.1</i> . |
| Viewing and Downloading Log Messages | Use the <b>Reports and Activity</b> pages.                                                                                                                                                                                                                               | See <a href="#">Viewing Log Messages, page A-10</a> .                                                                                                      |
| Troubleshooting with Log Messages    | Service log files reside in the <code>\Logs</code> subdirectory of the applicable service directory.                                                                                                                                                                     | See <a href="#">Debug Logs, page A-11</a> .                                                                                                                |







## AAA Protocols

This section contains the following topics:

- [Typical Use Cases, page B-1](#)
- [Access Protocols—TACACS+ and RADIUS, page B-5](#)
- [Overview of TACACS+, page B-5](#)
- [Overview of RADIUS, page B-6](#)

## Typical Use Cases

This section contains the following topics:

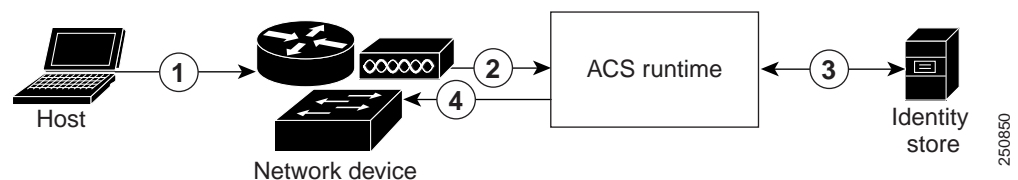
- [Device Administration \(TACACS+\), page B-1](#)
- [Network Access \(RADIUS With and Without EAP\), page B-2](#)

## Device Administration (TACACS+)

[Figure B-1](#) shows the flows associated with device administration. The two primary triggers are:

- [Session Access Requests \(Device Administration \[TACACS+\]\), page B-1.](#)
- [Command Authorization Requests, page B-2.](#)

*Figure B-1 Device Administration Flow*



## Session Access Requests (Device Administration [TACACS+])



Note

The numbers refer to [Figure B-1 Device Administration Flow, page B-1.](#)

For session request:

- 
- |               |                                                                                                                                                                                                                                |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | An administrator logs into a network device.                                                                                                                                                                                   |
| <b>Step 2</b> | The network device sends a TACACS+ access request to ACS.                                                                                                                                                                      |
| <b>Step 3</b> | ACS uses an identity store to validate the user's credentials.                                                                                                                                                                 |
| <b>Step 4</b> | ACS sends a TACACS+ response to the network device that applies the decision. The response includes parameters, such as the privilege level that determines the level of administrator access for the duration of the session. |
- 

## Command Authorization Requests



---

**Note** The numbers refer to [Figure B-1](#).

---

For command authorization:

- 
- |               |                                                                                                       |
|---------------|-------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | An administrator issues a command at a network device.                                                |
| <b>Step 2</b> | The network device sends a TACACS+ access request to ACS.                                             |
| <b>Step 3</b> | ACS optionally uses an identity store to retrieve user attributes for inclusion in policy processing. |
| <b>Step 4</b> | The TACACS+ response indicates whether the administrator is authorized to issue the command.          |
- 

## Network Access (RADIUS With and Without EAP)

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 ACS to authenticate and authorize the user.

ACS 5.8.1 supports the following categories of network access flows, depending on the protocol that is transported over the RADIUS protocol:

- RADIUS-based protocols that do not include EAP:
  - PAP
  - CHAP
  - MSCHAPv1
  - MSCHAPv2

For more information on RADIUS-based protocols that do not include EAP, see [RADIUS-Based Flow Without EAP Authentication, page B-3](#).

- EAP family of protocols transported over RADIUS, which can be further classified as:
  - Simple EAP protocols that do not use certificates:  
EAP-MD5  
LEAP

- EAP protocols that involve a TLS handshake and in which the client uses the ACS server certificate to perform server authentication:

PEAP, using one of the following inner methods: PEAP/EAP-MSCHAPv2 and PEAP/EAP-GTC

EAP-FAST, using one of the following inner methods: EAP-FAST/EAP-MSCHAPv2 and EAP-FAST/EAP-GTC

- EAP protocols that are fully certificate-based, in which the TLS handshake uses certificates for both server and client authentication:

EAP-TLS

PEAP with inner method EAP-TLS

For more information on RADIUS-based flows with EAP authentication, see [RADIUS-Based Flows with EAP Authentication](#), page B-3.

## RADIUS-Based Flow Without EAP Authentication

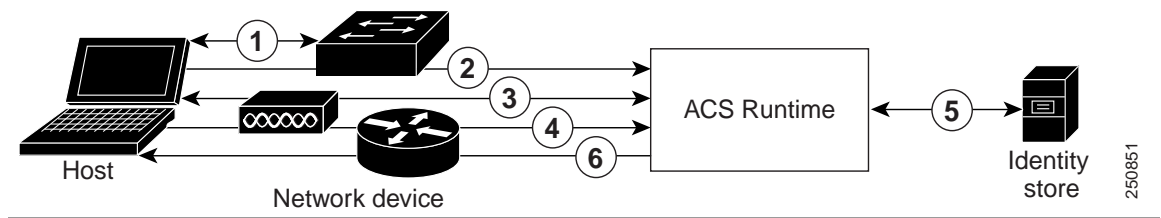
This section describes RADIUS-based workflow without EAP authentication.

For RADIUS with PAP authentication:

- 
- Step 1** A host connects to a network device.
- Step 2** The network device sends a RADIUS Access-Request to ACS, containing RADIUS attributes appropriate to the specific protocol that is being used (PAP, CHAP, MSCHAPv1, or MSCHAPv2).
- Step 3** ACS uses an identity store to validate the user's credentials.
- Step 4** The RADIUS response (Access-Accept or Access-Reject) is sent to the network device that will apply the decision.

[Figure B-2](#) shows a RADIUS-based authentication without EAP.

**Figure B-2** RADIUS-Based Flow Without EAP Authentication



## RADIUS-Based Flows with EAP Authentication

EAP provides an extensible framework that supports a variety of authentication types. Among them, the specific EAP methods supported by ACS are:

- Simple EAP methods that do not use certificates:
  - EAP-MD5
  - LEAP
- EAP methods in which the client uses the ACS server certificate to perform server authentication:
  - PEAP/EAP-MSCHAPv2

- PEAP/EAP-GTC
- EAP-FAST/EAP-MSCHAPv2
- EAP-FAST/EAP-GTC
- EAP methods that use certificates for both server and client authentication
  - EAP-TLS
  - PEAP/EAP-TLS

Whenever EAP is involved in the authentication process, it is preceded by an EAP negotiation phase to determine which specific EAP method (and inner method, if applicable) should be used.

For all EAP authentications:

- 
- Step 1** A host connects to a network device.
  - Step 2** The network device sends an EAP Request to the host.
  - Step 3** The host replies with an EAP Response to the network device.
  - Step 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 ACS.
  - Step 5** ACS 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.
  - Step 6** The network device extracts the EAP Request and sends it to the host.
- 

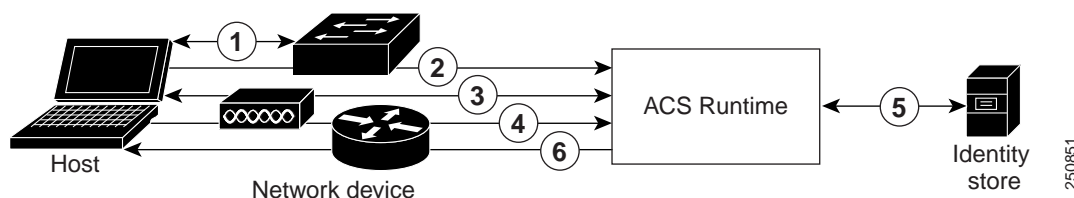
In this way, the host and ACS indirectly exchange EAP messages (transported over RADIUS and passed through the network device). The initial set of EAP messages that are exchanged in this manner negotiate the specific EAP method that will subsequently be used to perform the authentication.

The EAP messages that are subsequently exchanged are then used to carry the data needed to perform the actual authentication. If required by the specific EAP authentication method that is negotiated, ACS uses an identity store to validate the user's credentials.

After ACS 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).

Figure B-3 shows a RADIUS-based authentication with EAP.

**Figure B-3** RADIUS-Based Authentication with EAP



For a list of known supplicant issues that might impact your ACS 5.8.1 experience, see [Release Notes for Cisco Secure Access Control System 5.8.1](#).

# Access Protocols—TACACS+ and RADIUS

This section contains the following topics:

- [Overview of TACACS+, page B-5](#)
- [Overview of RADIUS, page B-6](#)

ACS 5.8.1 can use the TACACS+ and RADIUS access protocols. [Table B-1](#) compares the two protocols.

**Table B-1** TACACS+ and RADIUS Protocol Comparison

| Point of Comparison          | TACACS+                                                                                   | RADIUS                                                                                                                                                                                              |
|------------------------------|-------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Transmission Protocol</b> | TCP—Connection-oriented transport-layer protocol, reliable full-duplex data transmission. | UDP—Connectionless transport-layer protocol, datagram exchange without acknowledgments or guaranteed delivery. UDP uses the IP to get a data unit (called a datagram) from one computer to another. |
| <b>Ports Used</b>            | 49                                                                                        | Authentication and Authorization: 1645 and 1812<br>Accounting: 1646 and 1813.                                                                                                                       |
| <b>Encryption</b>            | Full packet-body encryption.                                                              | Encrypts only passwords up to 16 bytes.                                                                                                                                                             |
| <b>AAA Architecture</b>      | Separate control of each service: authentication, authorization, and accounting.          | Authentication and authorization combined as one service.                                                                                                                                           |
| <b>Intended Purpose</b>      | Device management.                                                                        | User access control.                                                                                                                                                                                |

## Overview of TACACS+

TACACS+ must be used if the network device is a Cisco device-management application, access server, router, or firewall. ACS 5.8.1 supports IPv6 addresses in TACACS+ protocols. ACS 5.8.1 supports Cisco device-management applications by providing command authorization for network users who are using the management application to configure managed network devices.

You provide support for command authorization for management application users by using unique command sets for each management application that is configured to use ACS for authorization.

ACS 5.8.1 uses TACACS+ to communicate with management applications. For a management application to communicate with ACS, you must configure the management application in ACS 5.8.1 as a AAA client that uses TACACS+.

You must also provide the device-management application with a valid administrator name and password. When a management application initially communicates with ACS, these requirements ensure the validity of the communication.

Except for the packet-headers, all information that the client and TACACS+ server communicate, which is contained in the packet-bodies are encrypted through the use of a shared secret (which is, itself, not sent over the network directly).

Additionally, the administrator that the management application uses must have the Command Set privilege enabled.

# Overview of RADIUS

This section contains the following topics:

- [RADIUS VSAs, page B-6](#)
- [ACS 5.8.1 as the AAA Server, page B-7](#)
- [RADIUS Attribute Support in ACS 5.8.1, page B-8](#)
- [RADIUS Access Requests, page B-10](#)

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. A company could use RADIUS to maintain user profiles in a central database that all remote servers can share.

This protocol provides better security, and the company can use it to set up a policy that is applied at a single administered network point.

To support the older and newer RFCs, ACS 5.8.1 accepts authentication requests on port 1645 and port 1812. For accounting, ACS accepts accounting packets on ports 1646 and 1813.

## RADIUS IETF

ACS 5.8.1 provides a set of standard IETF RADIUS attributes with a set of predefined sub-attributes and values. You can not edit these RADIUS IETF attributes. You can use them in policy conditions. You can identify RADIUS IETF attributes that are currently unused by their names. These unused attributes are named in the following format: *attribute-nnn*, where *attribute* is the name of the attribute and *nnn* is the ID of the attribute.

In ACS 5.8.1, you have two new sub-attributes for the RADIUS IETF attribute “Service Type” and they are:

- **HP-Oper** and its ID is 252
- **HP-User** and its ID is 255

You can use these two sub-attributes in policy conditions. These two sub-attributes are specifically designed for the HP devices to understand permissions of the user.

## RADIUS VSAs

ACS 5.8.1 supports RADIUS VSAs. The following set of predefined RADIUS VSAs are available after you install ACS 5.8.1:

- Cisco
- Cisco VPN 5000
- Microsoft
- US Robotics
- Ascend
- Nortel (Bay Networks)
- RedCreek
- Juniper

- Cisco VPN 3000
- Cisco Business Service Management (BSM)
- Cisco Aironet
- Cisco Airespace

You can modify these predefined RADIUS VSAs or define new RADIUS VSAs. You can create, edit, and duplicate RADIUS VSAs. For more information, see [Creating, Duplicating, and Editing RADIUS Vendor-Specific Attributes](#), page 18-7.

## ACS 5.8.1 as the AAA Server

A AAA server is a server program that handles user requests for access to computer resources, and for an enterprise, provides AAA services. The AAA server typically interacts with network access and gateway servers, and databases and directories that contain user information. The current standard by which devices or applications communicate with an AAA server is RADIUS.

ACS 5.8.1 functions as a AAA server for one or more network access devices (NADs). The NADs are clients of the ACS server. You must specify the IP address of ACS on each client NAD, to direct user access requests to ACS by using the RADIUS protocol.

RADIUS is universally used to secure the access of end-users to network resources. A RADIUS server can act as a proxy to other RADIUS servers or other kinds of authentication servers.

The NAD serves as the network gatekeeper and sends an Access-Request to ACS on behalf of the user. ACS verifies the username, password, and possibly other data by using either the internal identity store, or an externally configured LDAP or Windows Active Directory identity store.

ACS ultimately responds to the NAD with either an Access-Reject message or an Access-Accept message that contains a set of authorization attributes.

ACS 5.8.1 provides network transport over UDP and implements the RADIUS protocol, including RADIUS packet parsing and assembling, necessary data validation, and tracking of duplicate requests.

Some reasons for using UDP are:

- The processing time is only a few seconds.
- No special handling is required for rebooting or offline clients and servers.
- UDP is a connectionless protocol.
- UDP easily implements multithreaded servers to serve multiple client requests.

The UDP-assigned port number for RADIUS are:

- 1812 for access requests
- 1813 for accounting
- 1645 for access requests
- 1646 for accounting

ACS 5.8.1 is the entrance point to the authentication system. ACS listens on specific configurable UDP ports. When data arrives from the network:

- 
- |               |                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | ACS tries to process the data as a RADIUS client request or proxy response packet.                                                        |
| <b>Step 2</b> | ACS verifies that the packet arrived from the NAD that is registered in the configuration, and then prevents duplicate packet processing. |

- Step 3** ACS parses the RADIUS packet and performs the necessary validations of its contents.
- Step 4** ACS then passes the data for processing to the appropriate flow.
- Step 5** When the system is ready to respond, ACS:
- Receives the result of the data processing.
    - Creates a corresponding response to the client.
    - Returns the response to the network.
- 

## RADIUS Attribute Support in ACS 5.8.1

ACS 5.8.1 supports the RADIUS protocol as RFC 2865 describes.

ACS 5.8.1 supports the following types of RADIUS attributes:

- IETF RADIUS attributes
- Generic and Cisco VSAs
- Other vendors' attributes

ACS 5.8.1 also supports attributes defined in the following extensions to RADIUS:

- Accounting-related attributes, as defined in RFC 2866.
- Support for Tunnel Protocol, as defined in RFCs 2867 and 2868.
- Support for EAP (via the EAP-Message attribute), as defined in RFCs 2869 and 3579.



**Note**

When RADIUS parameters are referenced, the convention [*attribute-number*] [*attribute name*] is used. For example, [*1*]User-Name, where the number and name correspond to that assigned to the parameter in the specification.

---

RADIUS supports receiving, sending, and dictionary-based parsing and construction of any RADIUS attribute regardless of whether it is a regular attribute, VSA, or Cisco attribute-value (AV) pair. The RADIUS interface in ACS supports the attribute data types defined in RFC 2865, namely:

- *text* (UTF-8)
- *string* (binary)
- *address* (IP)
- *integer*
- *time*

Data types, integer, string, and text enumerated (ENUM) specifications of allowed values are supported. Attribute values are checked against these when packet parsing and construction occur.

ACS uses the RADIUS State attribute (24) to identify a specific conversation. Each conversation has a unique ID. Every conversation is processed under a specific configuration version—the latest available version at the moment the conversation was initiated.



**Note**

The RADIUS State attribute (24) is not used for PAP authentication.

---



All transactions between the client and RADIUS server have their message integrity protected using the Request/Response Authenticator field inside each RADIUS packet, which makes use of a shared secret (that is, itself, not sent over the network directly).

In addition, some forms of RADIUS packets that include all of those that contain encapsulated EAP-Message attributes have the integrity of all of their RADIUS attributes additionally protected using a Message-Authenticator RADIUS attribute (that also makes use of the shared secret).

Furthermore, user passwords within the RADIUS packets sent between the client and RADIUS server are always encrypted to protect against the possibility that an unauthorized user on an insecure network could easily determine the password.

### Authentication

ACS supports various authentication protocols transported over RADIUS. The supported protocols that do not include EAP are:

- PAP
- CHAP
- MSCHAPv1
- MSCHAPv2

In addition, various EAP-based protocols can be transported over RADIUS, encapsulated within the RADIUS EAP-Message attribute. These can be further categorized with respect to whether or not, and to what extent, they make use of certificates. These include:

- EAP methods that do not use certificates:
  - EAP-MD5
  - LEAP
- EAP methods in which the client uses the ACS server certificate to perform server authentication:
  - PEAP/EAP-MSCHAPv2
  - PEAP/EAP-GTC
  - EAP-FAST/EAP-MSCHAPv2
  - EAP-FAST/EAP-GTC
- EAP methods that use certificates for both server and client authentication:
  - EAP-TLS
  - PEAP/EAP-TLS

### Authorization

Authorization is permitted according to the configured access policies.

### Accounting

You can use the accounting functions of the RADIUS protocol independently of the RADIUS authentication or authorization functions. You can use some of the RADIUS accounting functions to send data at the start and end of sessions, and indicate the amount of resources (such as time, packets, bytes, and so on) that you used during the session.

An ISP might use RADIUS access control and accounting software to meet special security and billing needs.

## RADIUS Access Requests

A user login contains a query (Access-Request) from the network access device to the RADIUS server and a corresponding response (Access-Accept or Access-Reject) from the server. The Access-Request packet contains the username, password, NAD IP address, and NAD port, and other relevant attributes.

When the RADIUS server receives the access-request from the NAD, it searches a database for the username. Depending on the result of the database query, an accept or reject is sent. A text message can accompany the access-reject message to indicate the reason for the refusal.

In RADIUS, authentication and authorization are coupled. If the RADIUS server finds the username and the password is correct, the RADIUS server returns an access-accept response, including a list of attribute-value pairs that describe the parameters to use for this session. This list of parameters sets the authorization rights for the user.

Typical parameters include:

- Service type
- Protocol type
- IP address to assign the user (static or dynamic)
- Access list to apply
- A static route to install in the NAD routing table

The configuration information in the RADIUS server defines which parameters to set on the NAD during installation.



## Authentication in ACS 5.8.1

---

Authentication verifies user information to confirm the user's identity. Traditional authentication uses a name and a fixed password. More secure methods use cryptographic techniques, such as those used inside the Challenge Authentication Handshake Protocol (CHAP), OTP, and advanced EAP-based protocols. ACS supports a variety of these authentication methods.

A fundamental implicit relationship exists between authentication and authorization. The more authorization privileges granted to a user, the stronger the authentication should be. ACS supports this relationship by providing various methods of authentication.

### Authentication Considerations

Username and password 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. Simple unencrypted username and password is not considered a strong authentication mechanism but can be sufficient for low authorization or privilege levels such as Internet access.

You should use encryption to reduce the risk of password capture on the network. Client and server access-control protocols such as TACACS+ and RADIUS encrypt passwords to prevent them from being captured within a network.

However, TACACS+ and RADIUS operate only between the AAA client and ACS. Before this point in the authentication process, unauthorized persons can obtain clear-text passwords; for example, in the following setups:

- The communication between an end-user client dialing up over a phone line
- An Integrated Services Digital Network (ISDN) line terminating at a network-access server
- Over a TELNET session between an end-user client and the hosting device

### Authentication and User Databases

ACS supports a variety of user databases. It supports the ACS internal database and several external user databases, including:

- Windows Active Directory
- LDAP
- RSA SecurID Servers
- RADIUS Identity Servers

This appendix describes the following:

- RADIUS-based authentication that does not include EAP:
  - [PAP, page C-2](#)
  - [CHAP, page C-32](#)
  - MSCHAPv1
  - [EAP-MSCHAPv2, page C-30](#)
- EAP family of protocols transported over RADIUS, which can be further classified as:
  - Simple EAP protocols that do not use certificates:  
EAP-MD5—For more information, see [EAP-MD5, page C-5](#).  
LEAP—For more information, see [LEAP, page C-32](#).  
– EAP protocols that involve a TLS-handshake and in which the client uses the ACS server certificate to perform server authentication:  
PEAP, using one of the following inner methods: PEAP/EAP-MSCHAPv2 and  
PEAP/EAP-GTC—For more information, see [PEAPv0/1, page C-14](#).  
EAP-FAST, using one of the following inner methods: EAP-FAST/EAP-MSCHAPv2 and  
EAP-FAST/EAP-GTC—For more information, see [EAP-FAST, page C-19](#).  
– EAP protocols that are fully certificate-based, in which the TLS handshake uses certificates for both server and client authentication:  
EAP-TLS—For more information, see [EAP-TLS, page C-5](#).  
PEAP with inner method EAP-TLS, see [PEAPv0/1, page C-14](#).
- [Certificate Attributes, page C-32](#)
- [Machine Authentication, page C-35](#)
- [Authentication Protocol and Identity Store Compatibility, page C-36](#)

For a list of known supplicant issues, see [Release Notes for Cisco Secure Access Control System 5.8.1](#).

## PAP

The Password Authentication Protocol (PAP) provides a simple method for a user to establish its identity by using a two-way handshake. The PAP password is encrypted with the shared secret and is the least sophisticated authentication protocol.

ACS checks the ID-Password pair against the external database, Identity Store, until ACS acknowledges the authentication or terminates the connection.

PAP is not a strong authentication method since it offers little protection from repeated trial-and-error attacks.



### Note

---

The RADIUS with PAP authentication flow includes logging of passed and failed attempts.

---

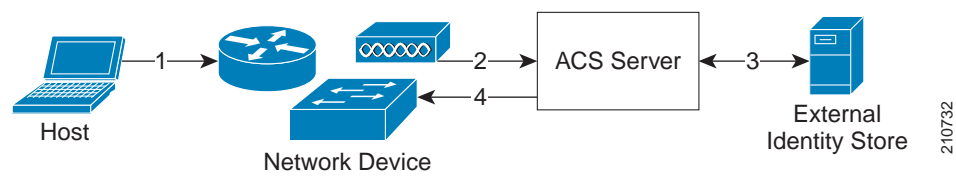
# RADIUS PAP Authentication

You can use different levels of security concurrently with ACS for different requirements. PAP applies a two-way handshaking procedure. If authentication succeeds, ACS returns an acknowledgment; otherwise, ACS 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.

Figure C-1 illustrates RADIUS with PAP authentication.

Figure C-1 RADIUS with PAP Authentication Use Case



|   |                                                                                               |   |                                                                                                                  |
|---|-----------------------------------------------------------------------------------------------|---|------------------------------------------------------------------------------------------------------------------|
| 1 | A host connects to the network. Any communication protocol may be used depending on the host. | 3 | ACS uses an external identity store to validate the user's credentials.                                          |
| 2 | The network device sends a RADIUS access request to ACS.                                      | 4 | The RADIUS response (Access-Accept or Access-Reject) is sent to the network device that will apply the decision. |

# EAP

Extensible Authentication Protocol (EAP) is an authentication framework for wireless networks and point-to-point connections. EAP supports multiple authentication methods, and provides common functions and rules for negotiation of the desired authentication method:

- Server authentication request
- Client authentication response
- Server success authentication result
- Server failure authentication result
- Silent discard of client packets if they do not meet integrity and security conditions
- Rules for server-initiated EAP method negotiation
- Message sequencing, and tracking responses to requests
- Retransmit

EAP is a lock-step protocol; after the initial request, ACS cannot send a new request before receiving a valid response from the client.

In ACS 5.8.1, EAP is encapsulated in the RADIUS protocol. Incoming and outgoing EAP messages are stored in a RADIUS EAP-Message attribute (79). A single RADIUS packet can contain multiple EAP-Message attributes when the size of a particular EAP message is greater than the maximum RADIUS attribute data size (253 bytes).

The RADIUS State attribute (24) stores the current EAP session reference information, and ACS stores the actual EAP session data.

The EAP standard is described in:

- RFC 3748—Extensible Authentication Protocol (EAP).
- RFC 3579—RADIUS Support For Extensible Authentication Protocol (EAP).

In the EAP process:

- 
- Step 1** The network device sends an EAP Request to a host when the host connects to the network.
- Step 2** The host sends an EAP Response to the network device; the network device embeds the EAP packet that it received from the host into a RADIUS request and sends it to ACS, which is acting as the EAP server.
- Step 3** ACS negotiates the EAP method for authentication. The client can acknowledge the EAP method that the EAP server suggests or, it can respond with a negative acknowledgment (NAK) and suggest a list of alternative EAP methods. The server and client must reach agreement about the EAP method to use to instantiate authentication.
- 

[Table C-1](#) lists the EAP codes for each type of EAP message.

**Table C-1** *EAP Codes*

| EAP message type | EAP code |
|------------------|----------|
| Accept-request   | 1        |
| Response         | 2        |
| Success          | 3        |
| Failure          | 4        |

[Table C-2](#) describes the EAP methods that ACS 5.8.1 supports.

**Table C-2** *Supported EAP methods*

| EAP Method   | Description                                                                                                                                           |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| EAP-MD5      | Message Digest 5 Protocol. For more information see <a href="#">EAP-MD5</a> , <a href="#">page C-5</a> .                                              |
| LEAP         | Lightweight Extensible Authentication Protocol.                                                                                                       |
| PEAPv0v1     | Protected Extensible Authentication Protocol version 0 and version 1. For more information see <a href="#">PEAPv0/1</a> , <a href="#">page C-14</a> . |
| EAP-FAST     | EAP Flexible Authentication via Secured Tunnel (EAP-FAST) protocol. For more information see <a href="#">EAP-FAST</a> , <a href="#">page C-19</a> .   |
| EAP-MSCHAPv2 | Microsoft Challenge Handshake Authentication Protocol version 2. For more information see <a href="#">EAP-MSCHAPv2</a> , <a href="#">page C-30</a> .  |

*Table C-2 Supported EAP methods (continued)*

| EAP Method | Description                                                                                                                               |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| EAP-GTC    | EAP Generic Token Card.                                                                                                                   |
| EAP-TLS    | Extensible Authentication Protocol-Transport Layer Security. For more information, see <a href="#">Exporting Credentials, page C-11</a> . |

ACS supports full EAP infrastructure, including EAP type negotiation, message sequencing and message retransmission. All protocols support fragmentation of big messages.

In ACS 5.8.1, you configure EAP methods for authentication as part of access service configuration. For more information about access services, see [ACS 5.x Policy Model, page 3-1](#)

## EAP-MD5

This section contains the following topics:

- [Overview of EAP-MD5, page C-5](#)
- [EAP- MD5 Flow in ACS 5.8.1, page C-5](#)

## Overview of EAP-MD5

EAP Message Digest 5-(EAP-MD5) provides one-way client authentication. The server sends the client a random challenge. The client proves its identity by hashing the challenge and its password with MD5. EAP-MD5 is vulnerable to dictionary attacks when it is used over an open medium.

This is because hackers are able to see the challenge and response. Since no server authentication occurs, it is also vulnerable to falsification.

### Related Topics

- [Host Lookup, page 4-12](#)
- [Overview of Agentless Network Access, page 4-12](#)

## EAP- MD5 Flow in ACS 5.8.1

ACS supports EAP-MD5 authentication against the ACS internal identity store. Host Lookup is also supported when using the EAP-MD5 protocol. See [Host Lookup, page 4-12](#).

### Related Topics

- [Authentication Protocol and Identity Store Compatibility, page C-36](#)
- [Overview of Agentless Network Access, page 4-12](#)

## EAP-TLS

This section contains the following topics:

- [Overview of EAP-TLS, page C-6](#)
- [EAP-TLS Flow in ACS 5.8.1, page C-13](#)

## Overview of EAP-TLS

EAP-TLS is one of the methods in the EAP authentication framework, and is based on the 802.1x and EAP architecture. Components involved in the 802.1x and EAP authentication process are the:

- Host—The end entity, or end user's machine.
- AAA client—The network access point.
- Authentication server—ACS.

The EAP-TLS standard is described in:

- RFC 2716—PPP EAP-TLS Authentication Protocol
- RFC 3079—Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)

This section contains the following topics:

- [User Certificate Authentication, page C-6](#)
- [PKI Authentication, page C-7](#)

The host must support EAP-TLS authentication. The access point must support the EAP authentication process in the 802.1x environment (the access point is not aware of the EAP authentication protocol type).

### Related Topics

- [Configuring CA Certificates, page 8-95](#)
- [Certificate-Based Network Access, page 4-8](#)
- [ACS and Cisco Security Group Access, page 4-22](#)
- [EAP-TLS Flow in ACS 5.8.1, page C-13](#)

## User Certificate Authentication

EAP-TLS is a mutual authentication method for certificate-based authentication; the client and server authenticate each other by using digital certificates. Certificates must meet specific requirements on the server and client for successful authentication. EAP and TLS are Internet Engineering Task Force (IETF) RFC standards.

The EAP protocol carries initial authentication information, specifically the encapsulation of EAP over LANs (EAPOL) as established by IEEE 802.1x. TLS uses certificates for user authentication and dynamic ephemeral session key generation.

After the peer is authenticated and a session is created, the information is cached on ACS for a certain amount of time. The session can be re-established by using the EAP-TLS session state and the session ticket resume, without an additional certificate exchange.

ACS 5.8.1 maintains the server certificate and private key in files on the ACS server, which it uses during EAP-TLS processing. You can choose the certificate authorities (CAs) that can be trusted to sign on client certificates.

EAP-TLS authentication involves two elements of trust:



- The EAP-TLS negotiation establishes end-user trust by validating, through RSA signature verifications, that the user possesses a keypair that a certificate signs.

This process verifies that the end user is the legitimate keyholder for a given digital certificate and the corresponding user identification in the certificate. However, trusting that a user possesses a certificate only provides a username-keypair binding.

- Using a third-party signature, usually from a CA, that verifies the information in a certificate. This third-party binding is similar to the real-world equivalent of the stamp on a passport.

You trust the passport because you trust the preparation and identity-checking that the particular country's passport office made when creating that passport. You trust digital certificates by installing the root certificate CA signature.

Some situations do not require this second element of trust that is provided by installing the root certificate CA signature. When such external validation of certificate legitimacy is not required, you can use the ACS self-signed certificate capability.

Depending on the end-user client involved, the CA certificate for the CA that issued the ACS server certificate is likely to be required in local storage for trusted root CAs on the end-user client computer. For more information, see [Adding a Certificate Authority, page 8-95](#).

EAP-TLS-compliant AAA clients include:

- Cisco 802.1x-enabled switch platforms (such as the Catalyst 6500 product line)
- Cisco Aironet Wireless solutions

To accomplish secure Cisco Aironet connectivity, EAP-TLS generates a dynamic, per-user, per-connection, unique session key.

ACS 5.8.1 now supports certificate name constraint extension. It accepts client certificates whose issuers contain the name constraint extension. It checks the client certificates for CA and sub-CA certificates. This extension defines a name space for all subject names in the subsequent certificates in a certificate path. It applies to both the subject distinguished name and the subject alternative name. These restrictions are applicable only when the specified name form is present in the client certificate. The ACS authentication fails if the client certificate is excluded or not permitted by the namespace.

#### Related Topics

- [Configuring CA Certificates, page 8-95](#)
- [Certificate-Based Network Access, page 4-8](#)

## PKI Authentication

EAP-TLS uses public key infrastructures (PKI) concepts:

- A host requires a valid certificate to authenticate to the LAN network.
- The AAA server requires a server certificate to validate its identity to the clients.
- The certificate-authority-server infrastructure issues certificates to the AAA server(s) and the clients.

An SSL/TLS tunnel authentication is conducted by both peers and is initiated by the client. In ACS, the tunnel can be either authenticated by:

- both peers
- either one
- neither client or host

A tunnel that is constructed without an authentication is considered an anonymous tunnel, and is usually constructed by the Diffie-Hellman key exchange protocol. ACS supports the SSL/TLS session resume feature for TLS. ACS maintains the tunnel keys and cipher used to establish the tunnel communication in the cache for each session. Fetching an old session is based on the session ID which is unique for each client.

You can configure the timeout for each session in the cache, for each protocol individually. The lifetime of a session is measured from the beginning of the conversation and is determined when the TLS session is created.

ACS supports establishment of a tunnel from a commonly shared key known to the client and the server for the EAP-FAST protocol. The key that is securely agreed upon between the two peers is used to derive a shared tunnel TLS-master-key that is used to open a tunnel. This mechanism involves a shorter TLS negotiation.

An anonymous Diffie-Hellman tunnel relates to the establishment of a completely anonymous tunnel between a client and a server for cases where none of the peers authenticates itself. ACS runtime supports anonymous Diffie-Hellman tunnels for EAP-FAST with a predefined prime and a predefined generator of two. There is no server authentication conducted within anonymous Diffie-Hellman tunnel cipher-suites.

An authenticated Diffie-Hellman tunnel is similar to an anonymous Diffie-Hellman tunnel. The additional factor of the authenticated Diffie-Hellman tunnel is that peer authentication is conducted through an RSA certificate. ACS supports Authenticated-Diffie-Hellman tunnels for EAP-FAST where the server authenticates by using its own certificate.

Additional client authentications are conducted within the tunnel by using other protocols, such as EAP-MSCHAPv2 or EAP-GTC for the inner EAP method.

#### Related Topics

- [Configuring Local Server Certificates, page 18-16](#)
- [Configuring CA Certificates, page 8-95](#)
- [Configuring Certificate Authentication Profiles, page 8-99](#)

## PKI Credentials

This section contains the following topics:

- [PKI Usage, page C-8](#)
- [Fixed Management Certificates, page C-9](#)
- [Importing Trust Certificates, page C-9](#)
- [Exporting Credentials, page C-11](#)

## PKI Usage

ACS supports using certificates for various PKI use cases. The main use case is the EAP-TLS protocol, where the PKI is used to authenticate not only the server, but also the client (PEAP and EAP-FAST also make use of certificates for server authentication, but do not perform client authentication). Other protocols which use the PKI credentials are LDAPS, HTTPS Management protocol, SSH, and SFTP.

For TLS related EAP protocols, a single local certificate is used to authenticate the server for all the TLS related EAP protocols. You can pick the certificate to use from any of the certificates containing a private-key in the Local Certificate store.

For other protocols, such as HTTPS, SFTP, and SSH, and for the message-bus ActiveMQ authentication, a single certificate should be configured to authenticate ACS. You can pick the certificate to use from any of the certificates containing a private-key in the Local Certificate store. You can configure the same local certificate for the TLS-related EAP protocols and for HTTPS Management protocol.

For HTTPS, SFTP, SSH and ActiveMQ, an auto-generated self-signed certificates can be used as the means for server authentication.

If ACS deployment is to be operated in FIPS mode, you must ensure that all local and certificate store 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.

## Fixed Management Certificates

ACS generates and uses self-signed certificates to identify various management protocols such as the Web browser, HTTPS, ActiveMQ SSH, and SFTP.

Self-signed certificates are generated when ACS is installed and are maintained locally in files outside of the ACS database. You cannot modify or export these certificates. You can, however, assign imported certificates to management interfaces.

## Importing Trust Certificates

ACS supports PEM or DER formatted X509 certificate files. You can add a trust certificate to the trust certificate store. ACS verifies that an imported certificate complies with the X509 format and does not perform any hierarchical certificate signature verification. ACS also supports the Microsoft proprietary private key format.

You can mark the acquired certificate for immediate trust for TLS related EAP protocols as the EAP CTL. The trust certificate store does not allow for duplicate trust certificates. These are the rules for rejecting certificates:

- Two certificates cannot have the same subject.
- Two certificates cannot have the same issuer and the same serial-number.

## Acquiring Local Certificates

This topic describes the methods for ACS to acquire PKI credentials, and the ways that you can set the public or private keys pairs to each ACS server in the ACS domain.

An X509 certificate contains the credentials which include the public key, and a PKCS#12 [?10.1] that holds the private key protected with a password that goes with it.

The ACS domain may have more than a single ACS server; each domain should have its own set of PKI key pairs to identify itself through the appropriate interfaces.

Some interfaces may require that the certificate that identifies ACS, contain the IP or FQDN of the ACS server, in its Common Name (CN) for better binding of the certificate to the IP of the server, for example, the HTTPS ACS server certificate which is used for the Web interface.

For other interfaces, it may be possible to use a common certificate that can be shared between the servers, however, Cisco does not recommend that you use a common certificate. Each ACS PKI credentials may be obtained either from a self-signed certificate or a certificate signed by a common certificate authority (CA).

For protocols that require the ACS identification, clients should be deployed with at least the lowest common certificate that dominates all the ACS servers certificates that are used to identify each ACS.

You can pick the PKI policy to be used in your organization and configure the PKI credentials for the ACS domain.

The configured certificate with its private-key should not be used outside the ACS machine

#### Related Topics

- [Importing the ACS Server Certificate, page C-10](#)
- [Initial Self-Signed Certificate Generation, page C-10](#)
- [Certificate Generation, page C-11](#)

## Importing the ACS Server Certificate

When you manually import an ACS server certificate you must supply the certificate file, the private key file, and the private key password used to decrypt the PKCS#12 private key. The certificate along with its private-key and private-key-password, is added to the Local Certificate store. For non-encrypted private-keys, the user supplied password may be ignored.

ACS supports PEM or DER formatted X509 certificate files. ACS verifies that an imported certificate complies with the X509 format and does not perform any hierarchical certificate signature verification.

When importing a certificate, you can configure the certificate for protocol that require an ACS server certificate, such as TLS related EAP protocols and HTTPS Management protocol.



#### Note

Only EAP and HTTPS Management protocols can be configured in ACS 5.8.1 for certificate-based authentication.

The input password and private-key, which are cryptographically sensitive information, are passed over the HTTPS channel. Using HTTPS with a non-authenticated server, for example, a self-signed certificate for HTTPS server authentication, is not a secure method of passing this sensitive information.



#### Note

If ACS is set to operate in FIPS mode, the certificate key size must be 2048 bits or greater in size and use either SHA-1 or SHA-256 hash algorithm.

#### Related Topics

- [Importing Trust Certificates, page C-9](#)
- [Initial Self-Signed Certificate Generation, page C-10](#)
- [Certificate Generation, page C-11](#)

## Initial Self-Signed Certificate Generation

An automatically generated, self-signed certificate is placed in the Local Certificate store for each ACS server. This certificate is used to identify ACS for TLS-related EAP protocols and for HTTPS Management protocols.

The self-signed certificate is generated with the CN equal to the machine's hostname, as required for HTTPS certificates, and is generated when ACS is installed.

## Certificate Generation

You can generate ACS server certificates through the Web interface. The output of this process is a certificate or a certificate request and its corresponding private-key and password. The generated private-key is structured as PKCS#12 encrypted, by using a relatively strong automatically generated password based on at least 128 bit of randomness.

You can select any of these generated private-key lengths: 512, 1024, 2048 or 4096 bit. The certificate digest algorithm used by the ACS is SHA1 and SHA2 256-bit.

**Note**

You should install Windows XP SP3 to use SHA2 256-bit certificates as management certificates.

There are two types of certificate generation:

- Self-signing certificate generation—ACS supports generation of an X.509 certificate and a PKCS#12 private key. The passphrase used to encrypt the private key in the PKCS#12 automatically generates stronger passwords, and the private key is hidden in the local certificate store.

You can select the newly generated certificate for immediate use for HTTPS Management protocol, for TLS-related EAP protocols, or both.

- Certificate request generation—ACS supports generation of a PKCS#10 certificate request with a PKCS#12 private key. The request is downloaded through the Web interface and should be formatted with PEM representation with a REQ extension.

The passphrase used to encrypt the private key in the PKCS#12 automatically generates stronger passwords, and the private-key is hidden in the ACS database. You can download the request file to be signed offline by the RA.

After the RA signs the request, you can install the returned signed certificate on ACS and bind the certificate with its corresponding private key. The binding of certificate and its private key is automatic.

After binding the signed certificate with the private key, you can mark this certificate for immediate use for HTTPS Management protocol, for TLS-related EAP protocols, or both.

### Related Topics

- [Configuring CA Certificates, page 8-95](#)
- [Configuring Certificate Authentication Profiles, page 8-99](#)
- [EAP-TLS Flow in ACS 5.8.1, page C-13](#)

## Exporting Credentials

You can export a general trust certificates, an ACS server certificate with or without private keys, and previously generated certificates requests from the certificate stores. You cannot export the request for a private-key. You can download certificates file with a *.CER* extension. The file format is not changed from the format that is imported into ACS.

You can download the public certificate as a regular certificate with *.CER* extension for ACS server certificates, that also contain a private key. The file format is retained.

You can export a public request to re-issue a certificate request to an RA, for certificate-requests. The request is downloaded with an REQ extension and is formatted identically to the format that it was generated by.

Only administrators with the highest administrator privileges can export the certificate private key and its password. A warning about the security implications of such an action is conveyed twice, to approve the export operation.

After this double check, the private-key files can be downloaded as a *.PVK* extension, and the private-key password can be downloaded as a *.PWD* extension. The private-key file format is retained.

## Credentials Distribution

All certificates are kept in the ACS database which is distributed and shared between all ACS nodes. The ACS server certificates are associated and designated for a specific node, which uses that specific certificate.

Public certificates are distributed along with the private keys and the protected private key passwords by using the ACS distributed mechanism. ACS implements a method of protection to prevent a private-key to be used by other servers other than the one to which the private-key is designated to. This protection mechanism applies only to encrypted private-keys.

The PKI policy for private keys is that private keys are not supposed to be usable by other entities which are not associated with the ACS server to which they are designated to. ACS supports cryptographic protection of the private-keys to prevent possible use outside of the ACS server machine to which they are designated to.

## Hardware Replacement and Certificates

When hardware fails, a new node is used for replacing a malfunctioning node. The malfunctioning node's certificates are removed from the distributed database of the primary server, and the new node's certificates are then being passed to the primary to be associated with the newly replaced node.

This process of certificate changing is conducted as part of the hardware replacement process when the new node registered to the domain. The certificate distribution is based on the server's IP address.

## Securing the Cryptographic Sensitive Material

There are several types of PKI-related keys that are stored in the ACS database. These keys have different cryptographic storage requirements that must comply to SEC-RCV-CRED-2 which is part of the Cisco security baseline. These requirements include:

- Public keys that usually reside in a certificate may be stored plain open as they are used to pass on the clear text to clients and contain only public keys.
- Private keys must be stored encrypted as PKCS#12 by using a relatively strong password.
- The password for the PKCS#12 private-keys must be stored in the ACS database. Since the ACS database is encrypted, this does not pose a serious security concern. ACS 5.8.1 distributes the entire database between all the ACS servers.

ACS encrypts the private-key passwords by using a password that exists only for the machine, thus preventing possible use of the private-keys by other machines. The private-key password key is maintained in */opt/CSCOacs/config/prikeypwd.key* on the ACS file-system.

Other certificate repositories such as the tomcat key-store should have the same properties as the ACS database. Private-keys are encrypted by a password that is kept secured in the database.

# Private Keys and Passwords Backup

The entire ACS database is distributed and backed-up on the primary ACS along with all the certificates, private-keys and the encrypted private-key-passwords. The private-key-password-key of the primary server is also backed up with the primary's backup.

Other secondary ACS private-key-password-keys are not backed-up. Backups are encrypted and also can pass relatively secured in and out of the ACS servers. The private keys in backups are protected by the PKCS#12 and the backup file encryption. The passwords that are used to open the PKCS#12 private-keys are protected with the backup encryption.

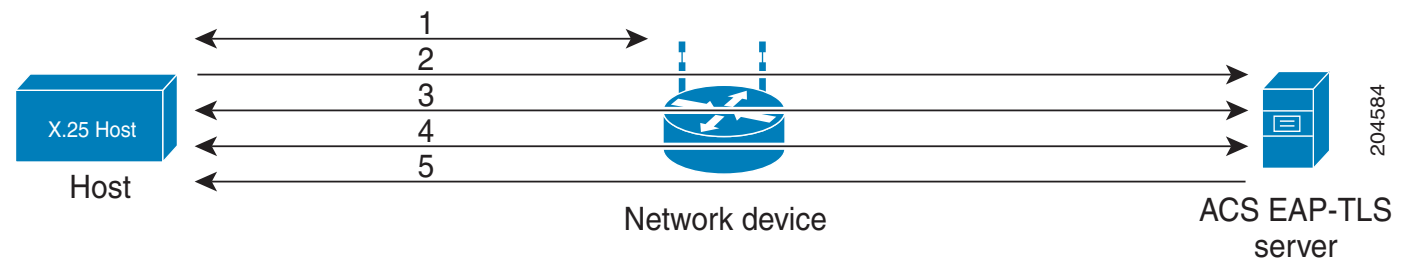
# EAP-TLS Flow in ACS 5.8.1

An EAP-TLS server exchanges data with a client by using packets based on the EAP Request and response packets; the packets are extended by specific EAP-TLS data. ACS acts as the EAP-TLS server and uses the Open Secure Sockets Layer (OpenSSL/CiscoSSL) library to process the TLS conversation. The ACS EAP-TLS server produces 128-bit MPPE send and receive keys that are used for encrypted communication between the client and server.

The ACS EAP-TLS server sends MPPE keys to the client in vendor-specific RADIUS attribute (26) by using vendor code Microsoft (311), and attributes MS-MPPE-Send-Key (16) and MS-MPPE-Recv-Key (17).

Figure C-2 shows the EAP-TLS processing flow between the host, network device, and ACS EAP-TLS server when the stateless session resume option is not used.

Figure C-2 EAP-TLS Flow



|   |                                                                                                                                                                                                          |   |                                                                                                                                                                                                                                                                       |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | A host connects to the network. The network device sends an EAP Request to the host.                                                                                                                     | 2 | The host sends an EAP Response to the network device; the network device embeds the EAP packet that it received from the host into a RADIUS Access-Request and sends it to ACS.                                                                                       |
| 3 | ACS negotiates the EAP method for authentication. The server and client must reach agreement to use EAP-TLS (EAP Request method 13) during EAP method negotiation to instantiate EAP-TLS authentication. | 4 | The client (host) and server (ACS) exchange certificates; this exchange involves several messages. EAP-TLS authentication is successful after the client and server have authenticated each other, and each side is aware that the other side has authenticated them. |
| 5 | ACS returns an EAP Success (or EAP Failure) message to the host and returns a RADIUS Access-Accept (or RADIUS Access-Reject) that includes session keys to the network device.                           |   |                                                                                                                                                                                                                                                                       |

**Note**

---

All communication between the host and ACS goes through the network device.

---

EAP-TLS authentication fails if the:

- Server fails to verify the client's certificate, and rejects EAP-TLS authentication.
- Client fails to verify the server's certificate, and rejects EAP-TLS authentication.

Certificate validation fails if the:

- Certificate has expired.
- Server or client cannot find the certificate issuer.
- Signature check failed.
- The client dropped cases resulting in malformed EAP packets.

EAP-TLS also supports the Session Resume feature. ACS supports the EAP-TLS session resume feature for fast reauthentication of a user who has already passed full EAP-TLS authentication. If the EAP-TLS configuration includes a session timeout period, ACS caches each TLS session for the duration of the timeout period.

When a user reconnects within the configured EAP-TLS session timeout period, ACS resumes the EAP-TLS session and reauthenticates the user with TLS handshake only, without a certificate check.

ACS 5.8.1 supports EAP-TLS session resumption without session state to be stored at the server. It also supports session ticket extension as described in RFC 5077. The ACS server creates a ticket and sends it to an EAP-TLS client. The client presents the ticket to ACS to resume a session.

The Stateless session resumption is supported in the distributed deployment, so that a session ticket issued by one node is accepted by another node.

The entire ticket is authenticated over its fields using a MAC with a 128-bit authentication key. The fields are encrypted using AES-CBC with a 128-bit encryption key and IV that are found in the ticket. The ACS administrator configures a limited lifetime for the session ticket.

**Related Topics**

- [Types of PACs, page C-23](#)
- [User Certificate Authentication, page C-6](#)

## PEAPv0/1

This section contains the following topics:

- [Overview of PEAP, page C-15](#)
- [EAP-MSCHAPv2, page C-30](#)

ACS 5.8.1 supports these PEAP supplicants:

- Microsoft Built-In Clients 802.1x XP (PEAPv0 only)
- Microsoft Built-In Clients 802.1x Vista (PEAPv0 only)
- Microsoft Built-In Clients 802.1x Windows 7
- CSSC v.4.0
- CSSC v.5



- Cisco AC 3.x
- Funk Odyssey Access Client 4.0.2 and 5.x
- Intel Supplicant 12.4.x

## Overview of PEAP

PEAP is a client-server security architecture that you use to encrypt EAP transactions, thereby protecting the contents of EAP authentications. PEAP uses server-side public key certificates to authenticate the server.

It then creates an encrypted SSL/TLS tunnel between the client and the authentication server. The ensuing exchange of authentication information to authenticate the client is then encrypted and user credentials are safe from eavesdropping.

PEAP is similar to EAP-TLS but uses a different client authentication method. PEAP provides authentication, by using server certificates, a TLS tunnel and client authentication through that encrypted tunnel. Unlike EAP-TLS, PEAP requires the client to use another EAP type, like EAP-MSCHAPv2.

PEAP authentications always involve two phases:

- In phase1, the end-user client authenticates ACS. This action requires a server certificate and authenticates ACS to the end-user client, ensuring that the user or machine credentials sent in phase two are sent to a AAA server that has a certificate issued by a trusted CA. The first phase uses a TLS handshake to establish an SSL tunnel between the end-user client and the AAA server.



### Note

Depending on the end-user client involved, the CA certificate for the CA that issued the ACS server certificate is likely to be required in local storage for trusted root CAs on the end-user client computer.

- In the second phase, ACS authenticates the user or machine credentials by using an EAP authentication protocol. The SSL tunnel that was created in phase1 protects the EAP authentication.

The inner-method authentication type that is negotiated during phase 2 can be either EAP-MSCHAPv2, EAP-GTC or EAP-TLS. The combination of the outer PEAP method with a specific inner EAP method is denoted using brackets (); for example, PEAP(EAP-MSCHAPv2) or PEAP(EAP-GTC).

An improvement in security that PEAP offers is identity protection. This improvement is the potential for protecting the username in all PEAP transactions. After phase one of PEAP, all data is encrypted, including username information that is usually sent in clear text.

The Microsoft PEAPv0 client does not provide identity protection; the Microsoft PEAPv0 client sends the username in clear text in phase one of PEAP authentication.

In ACS 5.8.1, PEAP is encapsulated in RADIUS protocol. Inner-method EAP messages are encapsulated in an EAP-TLV method. ACS also supports cryptobinding TLV extension in MS PEAP. In ACS 5.8.1, you have an option to deliberately enable PEAPv0 only for the legacy clients.

## Supported PEAP Features

This section contains the following topics:

- [Server Authenticated and Unauthenticated Tunnel Establishment Modes, page C-16](#)

- [Fast Reconnect, page C-16](#)
- [Session Resume, page C-16](#)
- [Protected Exchange of Arbitrary Parameters, page C-17](#)
- [Cryptobinding TLV Extension, page C-17](#)

## Server Authenticated and Unauthenticated Tunnel Establishment Modes

Tunnel establishment helps prevent an attacker from injecting packets between the client and the network access server (NAS) or, to allow negotiation of a less secure EAP method. The encrypted TLS channel also helps prevent denial of service attacks against the ACS.

A 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 RADIUS Access-Accept message.

The EAP Failure message is always carried in the RADIUS Access-Reject message. The client's PEAP message may cause the RADIUS client's message to drop unless the policy component is configured otherwise.

## Fast Reconnect

When a session resumes, another method of decreasing the authentication time is to skip the inner method, also known as fast reconnect. After a tunnel is built, the authentication flow goes directly to exchange authentication information with a Result TLV Success (v0)/tunneled EAP Success message for successful authentication and an EAP Failure message in case of unsuccessful authentication.

You can configure ACS to enable the fast reconnect option. After successful authentication, the client is able to perform a fast reconnect during a certain timeframe. PEAP fast reconnect reduces the delay in the time between an authentication request by a client and the response by ACS.

Fast reconnect also allows wireless clients to move between access points without repeated requests for authentication, which reduces resource requirements for the client and the server.

The user identity and the protocol used for user authentication (inner method) should be cached along with the TLS session to allow fast reconnect.

## Session Resume

ACS supports a session resume feature for PEAP-authenticated user sessions. When this feature is enabled, ACS caches the TLS session that is created during phase one of PEAP authentication, provided that the user successfully authenticates in phase two of PEAP.

If a user needs to reconnect and the original PEAP session has not timed out, ACS uses the cached TLS session, resulting in faster PEAP performance and a lessened AAA server load.

ACS stores the session in the cache after a successful full authentication. A client may try to resume the same session during a specific timeframe. A server certificate is not presented and the tunnel is built by using the session information from the OpenSSL/CiscoSSL session cache. The authentication flow then goes directly to the inner method.

If a client attempts to perform session resume but the timeout elapsed, ACS reverts to the full authentication flow.

You can configure the session resume and timeout values.

## Protected Exchange of Arbitrary Parameters

TLV tuples provide a way to exchange arbitrary information between the peer and ACS within a secure channel.

## Cryptobinding TLV Extension

The cryptobinding TLV extension in MS PEAP authentication is used to ensure that both the EAP peer (client) and the EAP server (ACS) are participating in the inner and outer EAP authentications of the PEAP authentication.

This cryptobinding process takes place as a two-way handshake between the PEAP server and PEAP peer. It consists of two messages, which include the cryptobinding request that is sent from a PEAP server to the PEAP peer and the cryptobinding response that is sent back from the PEAP peer to the PEAP server. This feature is implemented in ACS as primary for the MS Win 7 supplicant.

The TLV contains a compound MAC that is calculated using the following: PRF based on HMAC-SHA1-160 with TLV body as input data, a key derived from the PEAP tunnel key, and the inner method as session key. ACS verifies that the cryptobinding response TLV is received from the client. If the compound MAC is not equal to the expected data, then ACS fails the conversation. Cryptobinding is available for all inner methods. Cryptobinding is restricted to PEAPv0, because there are differences in protected termination flow. Cryptobinding is also applicable for PEAP session resume and fast reconnect. Some supplicants may not support cryptobinding TLV. If you send a cryptobinding TLV to a supplicant that does not support cryptobinding, then the supplicant does not provide a proper cryptobinding response. This improper response is considered to be an error on ACS and is accompanied with a PEAP\_CRYPTOBINDING\_FAILED message.

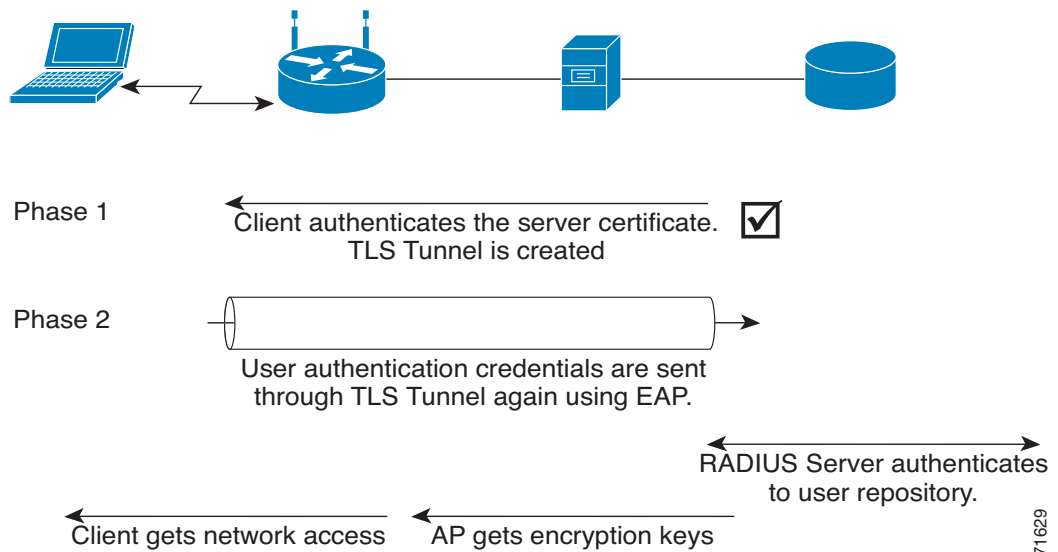
## PEAP Flow in ACS 5.8.1

The PEAP protocol allows authentication between ACS and the peer by using the PKI-based secure tunnel establishment and the EAP-MSCHAPv2 protocol as the inner method inside the tunnel. The local certificate can be validated by the peer (server-authenticated mode) or not validated (server-unauthenticated mode).

This section contains:

- [Creating the TLS Tunnel, page C-18](#)
- [Authenticating with MSCHAPv2, page C-18](#)

[Figure C-3](#) shows the PEAP processing flow between the host, access point, network device, and ACS EAP-TLS server.

**Figure C-3 PEAP Processing Flow**

271629

## Creating the TLS Tunnel

The following describes the process for creating the TLS tunnel:

|          |                                                                                                                                                                                                             |          |                                                                                                                                                                                                                               |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>1</b> | After creating a logical link, the wireless AP sends an EAP-Request/Identity message to the wireless client.                                                                                                | <b>2</b> | The wireless client responds with an EAP-Response/Identity message that contains the identity (user or computer name) of the wireless client.                                                                                 |
| <b>3</b> | The wireless AP sends the EAP-Response/Identity message to ACS. From this point on, the logical communication occurs between ACS and the wireless client by using the wireless AP as a pass-through device. | <b>4</b> | ACS sends an EAP-Request/Start PEAP message to the wireless client.                                                                                                                                                           |
| <b>5</b> | The wireless client and ACS exchange a series of TLS messages through which the cipher suite for the TLS channel is negotiated. In ACS 5.8.1, the client certificate is not used in PEAP.                   | <b>6</b> | At the end of the PEAP negotiation, ACS has authenticated itself to the wireless client. Both nodes have determined mutual encryption and signing keys (by using public key cryptography, not passwords) for the TLS channel. |

## Authenticating with MSCHAPv2

After the TLS tunnel is created, follow these steps to authenticate the wireless client credentials with MSCHAPv2:

|   |                                                                                                                                                                                         |   |                                                                                                                                                                        |
|---|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | ACS sends an EAP-Request/Identity message.                                                                                                                                              | 2 | The wireless client responds with an EAP-Response/Identity message that contains the identity (user or computer name) of the wireless client.                          |
| 3 | ACS sends an EAP-Request/EAP-MSCHAPv2 challenge message that contains a challenge string.                                                                                               | 4 | The wireless client responds with an EAP-Response/EAP-MSCHAPv2 Response message that contains the response to the ACS challenge string and a challenge string for ACS. |
| 5 | ACS sends an EAP-Request/EAP-MSCHAPv2 success message, which indicates that the wireless client response was correct and contains the response to the wireless client challenge string. | 6 | The wireless client responds with an EAP-Response/EAP-MSCHAPv2 acknowledgment message, indicating that the ACS response was correct.                                   |
| 7 | ACS sends an EAP-Success message.                                                                                                                                                       |   |                                                                                                                                                                        |

At the end of this mutual authentication exchange, the wireless client has provided proof of knowledge of the correct password (the response to the ACS challenge string), and ACS has provided proof of knowledge of the correct password (the response to the wireless client challenge string). The entire exchange is encrypted through the TLS channel created in PEAP.

#### Related Topics

- [Authentication Protocol and Identity Store Compatibility, page C-36](#)
- [Configuring PEAP Settings, page 18-3](#)

## EAP-FAST

This section contains the following topics:

- [Overview of EAP-FAST, page C-19](#)
- [EAP-FAST Flow in ACS 5.8.1., page C-27](#)
- [EAP-FAST PAC Management, page C-28](#)

## Overview of EAP-FAST

The EAP Flexible Authentication via Secured Tunnel (EAP-FAST) protocol is a new, publicly accessible IEEE 802.1x EAP type that Cisco developed to support customers that cannot enforce a strong password policy and want to deploy an 802.1x EAP type that does not require digital certificates.

EAP-FAST supports a variety of user and password database types, password change and expiration, and is flexible, easy to deploy, and easy to manage. For more information about EAP-FAST and comparison with other EAP types, see:

[http://www.cisco.com/en/US/products/hw/wireless/ps430/products\\_qanda\\_item09186a00802030dc.shtml](http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item09186a00802030dc.shtml).

EAP-FAST is a client-server security architecture that encrypts EAP transactions with a TLS tunnel. While similar to PEAP in this respect, it differs significantly in that EAP-FAST tunnel establishment is based on strong secrets that are unique to users.

These secrets are called Protected Access Credentials (PACs), which ACS generates by using a master key known only to ACS. Because handshakes based on shared secrets are intrinsically faster than handshakes based on PKI, EAP-FAST is the fastest of the advanced EAP protocols (including EAP-TLS and PEAP) that establish a TLS connection to encrypt the traffic between the supplicant and ACS. No certificate management is required to implement EAP-FAST.

EAP-FAST occurs in three phases:

- Phase zero—Unique to EAP-FAST, phase zero is a tunnel-secured means of providing an EAP-FAST end-user client with a PAC for the user requesting network access. (See [Automatic In-Band PAC Provisioning, page C-24.](#))

Providing a PAC to the end-user client is the sole purpose of phase zero. The tunnel is established based on an anonymous Diffie-Hellman key exchange for Anonymous In-band provisioning. Authenticated In-band provisioning uses other cipher suites.

If EAP-MSCHAPv2 or EAP-GTC authentication succeeds, ACS provides the user with a PAC. To determine which databases support EAP-FAST phase zero, see [Authentication Protocol and Identity Store Compatibility, page C-36.](#)



**Note** Phase zero is optional and PACs can be manually provided to end-user clients. (See [Manual PAC Provisioning, page C-24.](#))

The Allow Anonymous In-Band PAC provisioning option provides an end-user client with a PAC by using EAP-FAST phase zero. If this check box is checked, ACS establishes a secured connection with the end-user client for the purpose of providing the client with a new PAC.

This option allows an anonymous TLS handshake between the end-user client and ACS (EAP-MSCHAPv2 and EAP-GTC are used as inner methods.)

The Allow Authenticated In-Band PAC provisioning option provisions an end-user client with a PAC by using EAP-FAST phase zero with TLS server-side authentication. This option requires that you install a server certificate.

In general, phase zero of EAP-FAST does not authorize network access. However, if you choose the Accept Client on Authenticated Provisioning option, ACS sends a RADIUS Access-Accept (containing an EAP Success) at the end of a successful phase zero PAC provisioning, and the client is not forced to reauthenticate again.

This option can be enabled only when the Allow Authenticated In-Band PAC Provisioning option is also enabled.

- Phase one—In phase one, ACS and the end-user client establish a TLS tunnel based on the PAC that the end-user client presents. This phase requires that the end-user client has been provided a PAC for the user who is attempting to gain network access and that the PAC is not expired. The means by which PAC provisioning has occurred is irrelevant; you can use automatic or manual provisioning.
- Phase two—In phase two, ACS authenticates the user's credentials from within the protected TLS tunnel that was constructed in phase one, using EAP-MSCHAPv2 or EAP-GTC as the inner EAP method. To determine which databases support EAP-FAST phase two, see [Authentication Protocol and Identity Store Compatibility, page C-36.](#)

Phase one and phase two are subsequent parts of the same EAP-FAST conversation.

EAP-FAST can protect the username in all EAP-FAST transactions. ACS does not perform user authentication based on a username that is presented in phase one, however, whether the username is protected during phase one depends on the end-user client.

If the end-user client does not send the real username in phase one, the username is protected. After phase one of EAP-FAST, all data is encrypted, including username information that is usually sent in clear text.

ACS supports password aging with EAP-FAST for users who are authenticated by Windows user databases. Password aging can work with phase zero or phase two of EAP-FAST. If password aging requires a user to change passwords during phase zero, the new password would be effective in phase two.

## EAP-FAST Benefits

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 clear text or hashed, by the peer to the EAP server.
- **Immunity to man-in-the-middle (MitM) 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 MSCHAPv2 and 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 authentication server's per user authentication state requirements**—With large deployments, it is typical to have many servers acting as the authentication servers for many peers.

It is better for a peer to use the same shared secret to secure a tunnel much the same way 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 it must cache and manage.

## EAP-FAST in ACS 5.8.1

ACS supports in-band provisioning of the peer with a shared secret credential (PAC) based on PKI or ADHP (phase 0). Authentication of the peer and allowing the peer access to the network is implemented in phase 1 and phase 2.

ACS 5.8.1 supports EAP-FAST versions 1 and 1a.

This section contains the following topics:

- [About Master-Keys, page C-22](#)
- [About PACs, page C-22](#)
- [Provisioning Modes, page C-22](#)
- [Types of PACs, page C-23](#)
- [ACS-Supported Features for PACs, page C-25](#)
- [Master Key Generation and PAC TTLs, page C-26](#)
- [EAP-FAST for Allow TLS Renegotiation, page C-27](#)

## About Master-Keys

EAP-FAST master-keys are strong secrets that ACS automatically generates and of which only ACS is aware. Master-keys are never sent to an end-user client. EAP-FAST requires master-keys for two purposes:

- **PAC generation**—ACS generates PACs by using the active master-key. For details about PACs, see [About PACs, page C-22](#).
- **EAP-FAST phase one**—ACS determines whether the PAC that the end-user client presents was generated by one of the master-keys it is aware of.

To increase the security of EAP-FAST, ACS changes the master-key that it uses to generate PACs. ACS uses Master Key Generation Period values that you define to determine when it generates a new master-key and the age of all master-keys.

An active master-key is the master-key used by ACS to generate PACs. The Master Key Generation Period setting determines the duration that a master-key remains active. At any time, only one master-key is active. For more information about how TTL values determine whether PAC refreshing or provisioning is required, see [Master Key Generation and PAC TTLs, page C-26](#).

## About PACs

PACs are strong shared secrets that enable ACS and an EAP-FAST end-user client to authenticate each other and establish a TLS tunnel for use in EAP-FAST phase two. ACS generates PACs by using the active master-key and a username.

PAC comprises:

- **PAC-Key**—Shared secret bound to a client (and client device) and server identity.
- **PAC Opaque**—Opaque field that the client caches and passes to the server. The server recovers the PAC-Key and the client identity to mutually authenticate with the client.
- **PAC-Info**—At a minimum, includes the Authority ID to enable the client to cache different PACs. Optionally, it includes other information such as the PACs expiration time.

An EAP-FAST end-user client stores PACs for each user accessing the network with the client. Additionally, a AAA server that supports EAP-FAST has a unique Authority ID. An end-user client associates a user's PACs with the Authority ID of the AAA server that generated them. PACs remove the need for PKI (digital certificates).

During EAP-FAST phase one, the end-user client presents the PAC that it has for the current user and Authority ID that ACS sends at the beginning of the EAP-FAST transaction. The means of providing PACs to end-user clients, known as PAC provisioning, are discussed in [Automatic In-Band PAC Provisioning, page C-24](#) and [Manual PAC Provisioning, page C-24](#).

Modifying the master key generation values does not affect already created PACs. Any modifications you make to the master key generation values specify the period when the next master keys are generated.

## Provisioning Modes

ACS supports out-of-band and in-band provisioning modes. The in-band provisioning mode operates inside a TLS tunnel raised by Anonymous DH or Authenticated DH or RSA algorithm for key agreement.



To minimize the risk of exposing the user's credentials, a clear text password should not be used outside of the protected tunnel. Therefore, EAP-MSCHAPv2 or EAP-GTC are used to authenticate the user's credentials within the protected tunnel. The information contained in the PAC is also available for further authentication sessions after the inner EAP method has completed.

EAP-FAST has been enhanced to support an authenticated tunnel (by using the server certificate) inside which PAC provisioning occurs. The new cipher suites that are enhancements to EAP-FAST, and specifically the server certificate, are used.

At the end of a provisioning session that uses an authenticated tunnel, network access can be granted because the server and user have authenticated each other.

ACS supports the following EAP methods inside the tunnel for provisioning:

- EAP-MSCHAPv2
- EAP-GTC

By default, when you use EAP-MSCHAP inner methods, ACS allows authentication attempts up to the specified value you configured on the Service page inside the TLS tunnel if the initial authentication attempt fails. After the fourth failed authentication attempt inside the SSL tunnel, ACS terminates the EAP conversation, resulting in a RADIUS Access-Reject.

ACS supports issuing an out-of-band PAC file that allows you to generate a PAC that can be downloaded to ACS.

## Types of PACs

ACS supports the following types of PACs:

- Tunnel v1 and v1a
- SGA
- Machine
- Authorization

ACS provisions supplicants with a PAC that contains a shared secret that is used in building a TLS tunnel between the supplicant and ACS. ACS provisions supplicants with PACs that have a wider contextual use.

The following types of PACs are provisioned to ACS, as per server policies:

- **Tunnel/Machine PAC**—Contains user or machine information, but no policy information.
- **User Authorization PAC**—Contains policy elements (for example, inner method used for user authentication). You can use the User Authorization PACs to allow a stateless server session to resume, as described in [Session Resume, page C-16](#).

The various means by which an end-user client can receive PACs are:

- **PAC provisioning**—Required when an end-user client has no PAC. For more information about how master-key and PAC states determine whether PAC provisioning is required, see [Master Key Generation and PAC TTLs, page C-26](#).

The two supported means of PAC provisioning are:

- **Automatic In-Band PAC Provisioning**—Sends a PAC by using a secure network connection. For more information, see [Automatic In-Band PAC Provisioning, page C-24](#).
- **Manual provisioning**—Requires that you use ACS to generate a PAC file for the user, copy the PAC file to the computer that is running the end-user client, and import the PAC file into the end-user client. For more information, see [Manual PAC Provisioning, page C-24](#).

- **PAC refresh**—Occurs based on the value you specify in the Proactive PAC Update When field. For more information about how master-key and PAC states determine whether a PAC is refreshed, see [Master Key Generation and PAC TTLs, page C-26](#).

PACs have the following two states, which the PAC TTL setting determines:

- **Active**—A PAC younger than the PAC TTL is considered active and can be used to complete EAP-FAST phase one.
- **Expired**—A PAC that is older than the PAC TTL is considered expired. At the end of EAP-FAST phase two, ACS generates a new PAC for the user and provides it to the end-user client.

## Automatic In-Band PAC Provisioning

Automatic In-Band PAC Provisioning, which is the same as EAP-FAST phase zero, sends a new PAC to an end-user client over a secured network connection. Automatic In-Band PAC Provisioning requires no intervention of the network user or an ACS administrator, provided that you configure ACS and the end-user client to support Automatic In-Band PAC Provisioning.



### Note

Given that ACS associates each user with a single identity store, the use of Automatic In-Band PAC Provisioning requires that EAP-FAST users be authenticated with an identity store that is compatible with EAP-FAST phase zero. For the databases with which ACS can support EAP-FAST phase zero and phase two, see [Authentication Protocol and Identity Store Compatibility, page C-36](#).

In general, phase zero of EAP-FAST does not authorize network access. In this general case, after the client has successfully performed phase zero PAC provisioning, the client must send a new EAP-FAST request in order to begin a new round of phase one tunnel establishment, followed by phase two authentication.

However, if you choose the Accept Client on Authenticated Provisioning option, ACS sends a RADIUS Access-Accept (that contains an EAP Success) at the end of a successful phase zero PAC provisioning, and the client is not forced to reauthenticate again. This option can be enabled only when the Allow Authenticated In-Band PAC Provisioning option is also enabled.

Because transmission of PACs in phase zero is secured by MSCHAPv2 authentication, when MSCHAPv2 is vulnerable to dictionary attacks, we recommend that you limit use of Automatic In-Band PAC Provisioning to initial deployment of EAP-FAST.

After a large EAP-FAST deployment, PAC provisioning should be done manually to ensure the highest security for PACs. For more information about manual PAC provisioning, see [Manual PAC Provisioning, page C-24](#).

To control whether ACS performs Automatic In-Band PAC Provisioning, use the options on the Global System Options pages in the System Administration drawer. For more information, see [EAP-FAST, page C-19](#).

## Manual PAC Provisioning

Manual PAC provisioning requires an ACS administrator to generate PAC files, which must then be distributed to the applicable network users. Users must configure end-user clients with their PAC files.

You can use manual PAC provisioning to control who can use EAP-FAST to access your network. If you disable Automatic In-Band PAC Provisioning, any EAP-FAST user who is not provisioned with a PAC will not be able to access the network.

If your ACS deployment includes network segmentation, wherein a separate ACS controls access to each network segment, manual PAC provisioning enables you to grant EAP-FAST access on a per-segment basis.

For example, if your company uses EAP-FAST for wireless access in its Chicago and Boston offices and the Cisco Aironet Access Points at each of these two offices are configured to use different ACSs, you can determine, on a per-employee basis, whether Boston employees visiting the Chicago office can have wireless access.

While the administrative overhead of manual PAC provisioning is much greater than that of automatic in-band PAC provisioning, it does not risk sending the PAC over the network. Although manually provisioning the PACs requires a lot of effort early on, in configuring many end-user clients during the initial deployment, this type of provisioning is the most secure means for distributing PACs.

We recommend that, after a large EAP-FAST deployment, you manually perform PAC provisioning to ensure the highest security for PACs.

You can generate PAC files for specific usernames. You can also generate a PAC for a machine and provision the PAC manually to the client.

The following parameters are required to create a PAC:

- Specifying whether it is a user or machine PAC.
- Identity stored in Internal Identity Store ID field.
- PAC Time to Live (TTL).
- PAC encryption on or off, and password for encryption.

The PAC could be encrypted with the specified password by using the RC4 or AES algorithm. The detailed decryption algorithm must be provided to the client to allow decryption of the manually received PAC data.

## ACS-Supported Features for PACs

ACS 5.8.1 support these features for PACs.

### Machine PAC Authentication

Machine PAC-based authentication allows the machine to gain restricted network access before user authentication.

### Proactive PAC Update

ACS proactively provides a new PAC to the client after successful authentication when a configured percentage of the PAC TTL remains. The tunnel PAC update is initiated by the server after the first successful authentication that is performed before the PAC expiration.

The proactive PAC update time is configured for the ACS server in the Allowed Protocols Page. This mechanism allows the client to be always updated with a valid PAC.



**Note**

---

There is no proactive PAC update for Machine and Authorization PACs.

---

### Accept Peer on Authenticated Provisioning

The peer may be authenticated during the provisioning phase.

### PAC-Less Authentication

With PAC-less EAP-FAST Authentication, you can run EAP-FAST on ACS without issuing or accepting any tunnel or machine-generated PAC. The secure tunnel may be established by using a certificate rather than a PAC. Some PACs may be long-lived and not updated, which may cause authentication and security problems.

When PAC-less EAP-FAST is enabled, requests for PACs are ignored. Authentication begins with EAP-FAST phase zero and all subsequent requests for PACs are ignored. The flow moves on to EAP-FAST phase two. ACS responds with a Success-TLV message, without a PAC.

If a client attempts to establish a tunnel with a PAC, ACS responds with a PAC Invalid message. The tunnel establishment does not occur, and an Access-Reject is sent. The host or supplicant can reattempt to connect.

Anonymous phase zero, also known as ADHP is not supported for PAC-less authentication since the protocol does not support rolling over to phase two. PAC-less EAP-Fast supports configuration and does not require a client certificate.

[Table C-3](#) displays the different types of PACs and the authentication and authorization methods you can use them for.

**Table C-3** *PAC Rules Summary*

| PAC Type                                 | Tunnel v1/v1a/SGA                                                                                          | Machine                                                                                                     | Authorization                                                                          |
|------------------------------------------|------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Provide PAC on request on provisioning   | Yes                                                                                                        | Yes                                                                                                         | Provide PAC on request on provisioning.                                                |
| Provide PAC on request on authentication | Yes                                                                                                        | Yes                                                                                                         | Only if the PAC was not used in this authentication.                                   |
| Proactive update                         | Yes                                                                                                        | No                                                                                                          | No                                                                                     |
| When PAC is expired                      | Reject, try to fall on TLS fall back, provide a new PAC after successful authentication only (tunnel PAC). | Reject, try to fall on TLS fall back, provide a new PAC after successful authentication only (machine PAC). | Reject and provide a new PAC after successful authentication only (authorization PAC). |
| Support ACS 3.x/4.x PACs                 | For Tunnel PAC v1/v1a only                                                                                 | Yes                                                                                                         | No                                                                                     |

### Related Topics

- [About PACs, page C-22](#)
- [Provisioning Modes, page C-22](#)
- [Types of PACs, page C-23](#)
- [Master Key Generation and PAC TTLs, page C-26](#)

## Master Key Generation and PAC TTLs

The values for master key generation and PAC TTLs determine their states, as described in [About Master-Keys, page C-22](#) and [Types of PACs, page C-23](#). Master key and PAC states determine whether someone requesting network access with EAP-FAST requires PAC provisioning or PAC refreshing.

### Related Topics

- [About PACs, page C-22](#)

- [Provisioning Modes, page C-22](#)
- [Types of PACs, page C-23](#)
- [ACS-Supported Features for PACs, page C-25](#)

## EAP-FAST for Allow TLS Renegotiation

You may be prompted to enter a password twice when you use an anonymous PAC provisioning schema. When you enter the password the first time, ACS provisions the PAC and sends an access-reject to the client. The client is then prompted to re-enter the password so that they will be able to authenticate and be granted access to the network.

ACS checks for a TLS client handshake record. If it finds the TLS client handshake record, ACS will initiate a TLS renegotiation at the end of EAP-Fast phase zero, instead of rejecting the user's request for access.

You should use this option with a Vista client when the host is using anonymous PAC provisioning. Vista client do not save the user password in the cache, so you are allowed to enter the password once. When this option is enabled, ACS initiates the TLS renegotiation request to the client at the end of EAP-FAST phase zero, instead of rejecting the access attempt after PAC provisioning.

## EAP-FAST Flow in ACS 5.8.1.



### Note

You must configure the end-user clients to support EAP-FAST. This procedure is specific to configuring ACS only.

### Before You Begin

The steps in this procedure are a suggested order only. Enabling EAP-FAST at your site may require recursion of these steps or performing these steps in a different order.

For example, in this procedure, determining how you want to support PAC provisioning comes after configuring a user database to support EAP-FAST; however, choosing Automatic In-Band PAC Provisioning places different limits on user database support.

To enable ACS to perform EAP-FAST authentication:

- 
- Step 1** Configure an identity store that supports EAP-FAST authentication.
- To determine which identity stores support EAP-FAST authentication, see [Authentication Protocol and Identity Store Compatibility, page C-36](#). For information about configuring identity stores, see [Managing Users and Identity Stores, page 8-1](#)
- Step 2** Determine master key generation and PAC TTL values.
- For information about how master key generation and PAC TTL values determine whether PAC provisioning or PAC refreshing is required, see [Master Key Generation and PAC TTLs, page C-26](#).
- Step 3** Determine whether you want to use automatic or manual PAC provisioning.
- For more information about the two means of PAC provisioning, see [Automatic In-Band PAC Provisioning, page C-24](#), and [Manual PAC Provisioning, page C-24](#).
- We recommend that you limit the use of Automatic In-Band PAC Provisioning to initial deployments of EAP-FAST, before you use manual PAC provisioning for adding small numbers of new end-user clients to your network and replacing PACs based on expired master keys.

- Step 4** Using the decisions during [Step 2 Determine master key generation and PAC TTL values., page C-27](#) and [Step 3 Determine whether you want to use automatic or manual PAC provisioning., page C-27](#), enable EAP-FAST in the Global Systems Options drawer. See [EAP-FAST, page C-19](#) for more information.
- ACS is ready to perform EAP-FAST authentication.

**Note**

Inner-identity will not be logged when: the workstation not allowed error appears, the SSL Handshake fails, EAP-PAC is provisioned, and ACS receives an invalid PAC.

**Related Topics**

- [Managing Internal Identity Stores, page 8-4](#)
- [Managing External Identity Stores, page 8-29](#)

## EAP-FAST PAC Management

The EAP-FAST master-key in ACS is used to encrypt or decrypt, sign and authenticate the PACs and PAC-Opaque's that are used by EAP-FAST to store server opaque data by a supplicant. EAP-FAST requires a distributed mechanism by which each server in the ACS domain is able to pack and unpack PACs securely, including those which were packed on a different server.

The EAP-FAST master-key must have a common secret that is known to all servers in the ACS domain. The master-key is periodically refreshed and keys are replaced securely and synchronized by all ACS servers. The keys are generated of high entropy to comply with strong cryptographic standards such as FIPS-140.

In previous versions of ACS, the master-key was distributed by the ACS distribution mechanism and was replaced from time to time to improve the security of those keys. ACS 5.8.1 introduces a new scheme that provides simplicity, correctness, robustness, and security for master -key distribution.

The ACS EAP-FAST new distribution scheme contains a secure way of distributing the common seed-key, from which each ACS server can deterministically derive the same set of master-keys. Each PAC contains the information that the master-key was derived from, and each server can securely reconstruct the master-key that encrypted and signed the PAC.

This scheme improves the security by reducing the amount of cryptographic sensitive material that is transmitted.

This section contains the following topics:

- [Key Distribution Algorithm, page C-28](#)
- [EAP-FAST PAC-Opaque Packing and Unpacking, page C-29](#)
- [Revocation Method, page C-29](#)
- [PAC Migration from ACS 4.x, page C-29](#)

## Key Distribution Algorithm

The common seed-key is a relatively large and a completely random buffer that is generated by the primary ACS server. The seed-key is generated only once during installation, or it can be manually regenerated by an administrator. The seed-key should rarely be replaced, because if you change seed-key, of all the previous master-keys and PACs would automatically be deactivated.

The seed-key is generated by using a FIPS approved RNG generator that exists in the runtime cryptographic module (CryptoLib). The ACS primary server management determines when to generate the seed-key, and communicates with the ACS runtime to request a new seed-key to be generated.

The size of the seed-key may vary and should consist of at least 64 bytes (512 bit). A larger seed might have some performance implication as each master-key derivation is dependent on it subsequently.

At any given time, a single seed-key should be used by each ACS server and the primary ACS server should ensure to distribute the latest seed-key to all the servers. Old seed-keys must be discarded.

The seed-key contains critical cryptographic sensitive information. Disclosing the seed-key information would expose the entire EAP-FAST PAC mechanism to a large set of possible identity vulnerabilities.

Because of that, the mechanism which transports the seed-key between the primary and the secondary ACS servers must be fully secured. Further security measures must be taken with respect to storing the seed-key in the data-base. The seed-key should be protected with the strongest means of security.

## EAP-FAST PAC-Opaque Packing and Unpacking

When the server generates a new PAC, it must derive the master-key to be used. When the server accepts a new PAC the same algorithm should be used for deriving the master-key with some additional verification used to prevent possible attacks on the master-key scheme. The derivation calculation may be skipped if the master-key was already placed in the cache in the past.

## Revocation Method

You can revoke all PACs and all Master-Keys. For this type of extensive revocation, all you need to do is to revoke the seed-key and replace it by a new one.

Having only a single seed-key to be used in the system facilitates implementation.

## PAC Migration from ACS 4.x

Although the configuration can be migrated from 4.x, the PACs themselves, as being stored only in supplicants, may still be issued from versions as far back as ACS 3.x. ACS 5.8.1 accepts PACs of all types according to migrated master-keys from versions 4.x and onwards, and re-issues a new 5.0 PAC, similar to the proactive PAC update for EAP-FAST 5.0.

When ACS 5.8.1, accepts a PAC from either ACS 3.x or 4.x, it decrypts and authenticates the PAC according to the 4.x master-key that was migrated from ACS 4.x configuration. The decryption and handling of this type of PAC is similar to the way the ACS 4.x PAC was handled.

The migration process involves converting the following data-items:

- EAP-FAST A-ID of ACS (Authority ID). The parameter replaces the deployment's A-ID of ACS 5.8.1.
- A list of retired ACS 4.x master-keys. The list is taken from the ACS 4.x configuration and placed in a new table in ACS 5.8.1. Each migrated master-key is associated with its expected time of expiration. The table is migrated along with the master-key identifier (index) and the PAC's-cipher assigned to each key.

## EAP Authentication with RADIUS Key Wrap

You can configure ACS to use PEAP, EAP-FAST and EAP-TLS authentication with RADIUS Key Wrap. ACS can then authenticate RADIUS messages and distribute the session key to the network access server (NAS). The EAP session key is encrypted by using Advanced Encryption Standard (AES), and the RADIUS message is authenticated by using HMAC-SHA-1.

Because RADIUS is used to transport EAP messages (in the EAP-Message attribute), securely authenticating RADIUS messages ensures securely authenticated EAP message exchanges. You can use RADIUS Key Wrap when PEAP, EAP-FAST and EAP-TLS authentication is enabled as an external authentication method. Key Wrap is not supported for EAP-TLS as an inner method (for example, for EAP-FAST or PEAP).

RADIUS Key Wrap support in ACS uses three new AVPs for the cisco-av-pair RADIUS Vendor-Specific-Attribute (VSA); the TLV value of Cisco VSA is [26/9/1]):

- **Random-Nonce**—Generated by the NAS, it adds randomness to the key data encryption and authentication, and links requests and response packets to prevent replay attacks.
- **Key**—Used for session key distribution.
- **Message-Authenticator-Code**—Ensures the authenticity of the RADIUS message, including the EAP-Message and Key attributes.

While using RADIUS Key Wrap, ACS enforces the use of these three RADIUS Key Wrap AVPs for message exchanges and key delivery. ACS will reject all RADIUS (EAP) requests that contain both RADIUS Key Wrap AVPs and the standard RADIUS Message-Authenticator attribute.

To use RADIUS Key Wrap in PEAP, EAP-FAST and EAP-TLS authentications, you must enable the EAP authentication with RADIUS KeyWrap in the Network Devices and AAA Clients page or Default Network Device page.

You must also define two shared secret keys for each AAA Client. Each key must be unique and be distinct from the RADIUS shared key. RADIUS Key Wrap does not support proxy functionality, and should not be used with a proxy configuration.

## EAP-MSCHAPv2

Microsoft Challenge Handshake Authentication Protocol (MSCHAP v2) provides two-way authentication, also known as mutual authentication. The remote access client receives verification that the remote access server that it is dialing in to has access to the user's password.

This section contains the following topics:

- [Overview of EAP-MSCHAPv2, page C-30](#)
- [EAP- MSCHAPv2 Flow in ACS 5.8.1, page C-31](#)

## Overview of EAP-MSCHAPv2

Some of the specific members of the EAP family of authentication protocols, specifically EAP-FAST and PEAP, support the notion of an “EAP inner method.” This means that another EAP-based protocol performs additional authentication within the context of the first protocol, which is known as the “EAP outer method.”



One of the inner methods supported by the EAP-FAST and PEAP outer methods is EAP-MSCHAPv2, which is an adaptation of the MSCHAPv2 protocol that complies with the general framework established by EAP.

Using EAP-MSCHAPv2 as the inner EAP method facilitates the reuse of Microsoft directory technology (such as Windows Active Directory), with the associated database of user credentials for wireless authentication in the following contexts:

- [MSCHAPv2 for User Authentication, page C-31](#)
- [MSCHAPv2 for Change Password, page C-31](#)
- [Windows Machine Authentication Against AD, page C-31](#)

## MSCHAPv2 for User Authentication

ACS supports the EAP-MSCHAPv2 authentication protocol as the inner method of EAP-FAST and PEAP. The protocol is an encapsulation of MSCHAPv2 into the EAP framework. Mutual authentication occurs against the configured credential database.

The client does not send its password, but a cryptographic function of the password. Using EAP-MSCHAPv2 as the inner method of tunneling protocols, increases protection of secured communication. Every protocol message is encrypted inside the tunnel and server, and client challenges are not generated randomly but, derived from outer method cryptographic material.

EAP-MSCHAPv2 is supported for AD and the ACS internal identity store.

## MSCHAPv2 for Change Password

When you use EAP-MSCHAPv2 (as an EAP inner method) to authenticate a user whose password has expired, ACS sends a specific EAP-MSCHAPv2 failure notification to the client. The client can prompt the user for new password and then provide it to ACS inside the same conversation.

The new password is encrypted with the help of the old one. When a user password is changed successfully, the new user password is stored in the credential database.

EAP-MSCHAPv2 change password is supported for AD and ACS internal identity store.

## Windows Machine Authentication Against AD

EAP-MSCHAPv2 can be used for machine authentication. EAP-MSCHAPv2 Windows machine authentication is the same as user authentication. The difference is that you must use the Active Directory of a Windows domain, since a machine password can be generated automatically on the machine and the AD, as a function of time and other parameters. The password generated cannot be stored in other types of credential databases.

## EAP-MSCHAPv2 Flow in ACS 5.8.1

Components involved in the 802.1x and MSCHAPv2 authentication process are the:

- Host—The end entity, or end user's machine.
- AAA client—The network access point.
- Authentication server—ACS.

The MSCHAPv2 protocol is described in RFC 2759.

**Related Topic**

- [Authentication Protocol and Identity Store Compatibility, page C-36](#)

## CHAP

CHAP uses a challenge-response mechanism with one-way encryption on the response. CHAP enables ACS 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 ACS internal database for authentication, you can use PAP or CHAP. CHAP does not work with the Windows 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.

## LEAP

ACS currently uses 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 EAP-TLS, we recommend that you disable this option.

**Note**

---

If users who access your network by using a AAA client that is defined in the Network Configuration section as a RADIUS (Cisco Aironet) device, then you must enable LEAP, EAP-TLS, or both; otherwise, Cisco Aironet users cannot authenticate.

---

## Certificate Attributes

ACS parses the following client certificate's attributes:

- Certificate serial-number (in binary format)
- Encoded certificate (in binary DER format)
- Subject's CN attribute
- Subject's O attribute (Organization)
- Subject's OU attribute (Organization Unit)
- Subject's L attribute (Location)
- Subject's C attribute (Country)
- Subject's ST attribute (State Province)
- Subject's E attribute (eMail)
- Subject's SN attribute (Subject Serial Number)
- Issuer I attribute
- SAN (Subject Alternative Name)

You can define a policy to set the principle username to use in the TLS conversation, as an attribute that is taken from the received certificate.

The attributes that can be used as the principle username are:

- Subject CN
- Subject Serial-Number (SN)
- SAN
- Subject
- SAN—Email
- SAN—DNS
- SAN—otherName

If the certificate does not contain the configured attribute, authentication fails.



**Note**

---

ACS 5.8.1 supports short hard-coded attributes and certificate attribute verification for the only the EAP-TLS protocol.

---

## Certificate Binary Comparison

You can perform binary comparison against a certificate that ACS receives from an external identity store and determine the identity store's parameters that will be used for the comparison.



**Note**

---

In ACS 5.8.1, AD and LDAP are the only external identity stores that hold certificates.

---

ACS uses the configured principle username to query for the user's certificate and then perform binary comparison between the certificate received from external identity store and the one received from the client. The comparison is performed on a DER certificate format.

## Rules Relating to Textual Attributes

ACS collects client certificate textual attributes and places them in the ACS context dictionary. ACS can apply any rule based policy on these attributes as with any rule attributes in ACS.

The attribute that can be used for rule verification are:

- Subject's CN attribute
- Subject's O attribute (Organization)
- Subject's OU attribute (Organization Unit)
- Subject's L attribute (Location)
- Subject's C attribute (Country)
- Subject's ST attribute (State Province)
- Subject's E attribute (eMail)
- Subject's SN attribute (Subject Serial Number)
- Issuer I attribute
- SAN (Subject Alternative Name)
- Subject

- SAN—Email
- SAN—DNS
- SAN—otherName

## Certificate Revocation

Every client certificate that ACS receives is verified with a Certificate Revocation List (CRL) according to a policy that is defined.

The CRL mechanism verifies whether or not you can still rely on a client certificate. This is done by checking the serial number of the certificate, and that of each member of the corresponding certificate chain, against a list of certificates that are known to have been revoked.

Possible reasons for revocation of a certificate include suspicion that the associated private key has been compromised or the realization that the certificate was issued improperly. If either of these conditions exist, the certificate is rejected.

ACS supports a static-CRL that contains a list of URLs used to acquire the CRL files that are configured in ACS database.



**Note**

---

ACS does not support delta CRLs in certificate revocation validation.

---

You can configure a set of URLs used for CRL update for each trusted CA certificate,. By default, when adding a CA certificate, ACS automatically sets all the URLs stored in the certificate *crlDistributionPoint* as the initial static CRL for that CA. In most cases, the *crlDistributionPoint* is used to point to the CRL location used to revoke the CA certificate, but you can edit the URL to point to the CRL file issued by this CA. You can only configure a single HTTP based URL for each CA.

You can configure the parameters for each CA, which will apply to all the URLs that are configured to the CA. ACS supports two download modes, one for periodic download, and the other for downloading the next CRL update just before the previous is about to expire.

- For the periodic download, you can define the download periods.
- For automatic downloading, you define the amount of time before the CRL file expires, should ACS download it. The CRL expiration time is taken from the *CRL nextUpdate* field.

For both modes, if the download somehow fails, you can define the amount of time that ACS will wait before trying to redownload the CRL file.

ACS verifies that the downloaded CRL file is signed correctly by any one of the CAs in the trust store, for each downloaded CRL file and whether they are trusted. ACS uses the CRL file only if the signature verification passes. The verified CRL file replaces the previous CRL file issued by the same CA.



**Note**

---

CRL files are not kept persistent, and should be re-downloaded when you restart ACS.

---

The configuration of URLs and their association to CA's is distributed to the entire ACS domain. The downloaded CRLs are not distributed and are autonomously populated in parallel in each ACS server.

# Machine Authentication

ACS supports the authentication of computers that are running the Microsoft Windows operating systems that support EAP computer authentication. Machine authentication, also called computer authentication, allows networks services only for computers known to Active Directory.

This feature is especially useful for wireless networks, where unauthorized users outside the physical premises of your workplace can access your wireless access points.

When machine authentication is enabled, there are three different types of authentications. When starting a computer, the authentications occur in this order:

- **Machine authentication**—ACS authenticates the computer prior to user authentication. ACS checks the credentials that the computer provides against the Windows identity store.

If you use Active Directory and the matching computer account in AD has the same credentials, the computer gains access to Windows domain services.

- **User domain authentication**—If machine authentication succeeded, the Windows domain authenticates the user. If machine authentication failed, the computer does not have access to Windows domain services and the user credentials are authenticated by using cached credentials that the local operating system retains.

In this case, the user can log in to only the local system. When a user is authenticated by cached credentials, instead of the domain, the computer does not enforce domain policies, such as running login scripts that the domain dictates.

**Note**

If a computer fails machine authentication and the user has not successfully logged in to the domain by using the computer since the most recent user password change, the cached credentials on the computer will not match the new password. Instead, the cached credentials will match an older password of the user, provided that the user once successfully logged in to the domain from this computer.

- **User network authentication**—ACS authenticates the user, allowing the user to have network connectivity. If the user exists, the identity store that is specified is used to authenticate the user.

While the identity store is not required to be the Windows identity store, most Microsoft clients can be configured to automatically perform network authentication by using the same credentials used for user domain authentication. This method allows for a single sign-on.

**Note**

Microsoft PEAP clients may also initiate machine authentication whenever a user logs off. This feature prepares the network connection for the next user login. Microsoft PEAP clients may also initiate machine authentication when a user shuts down or restarts the computer rather than just logging off.

ACS supports EAP-TLS, EAP-FAST, PEAP (EAP-MSCHAPv2), and PEAP (EAP-GTC) for machine authentication. You can enable each separately on the Active Directory: General Page, which allows a mix of computers that authenticate with EAP-TLS, EAP-FAST, or PEAP (EAP-MSCHAPv2).

Microsoft operating systems that perform machine authentication might limit the user authentication protocol to the same protocol that is used for machine authentication.

**Related Topics**

- [Microsoft AD, page 8-52](#)
- [Managing External Identity Stores, page 8-29](#)

# Authentication Protocol and Identity Store Compatibility

ACS supports various authentication protocols to authenticate against the supported identity stores.

[Table C-4](#) specifies non-EAP authentication protocol support.

**Table C-4** *Non-EAP Authentication Protocol and User Database Compatibility*

| Identity Store        | ASCII/PAP | MSCHAPv1/MSCHAPv2 | CHAP |
|-----------------------|-----------|-------------------|------|
| ACS                   | Yes       | Yes               | Yes  |
| Windows AD            | Yes       | Yes               | No   |
| LDAP                  | Yes       | No                | No   |
| RSA Identity Store    | Yes       | No                | No   |
| RADIUS Identity Store | Yes       | No                | No   |

[Table C-5](#) specifies EAP authentication protocol support.

**Table C-5** *EAP Authentication Protocol and User Database Compatibility*

| Identity Store        | EAP-MD5 | EAP-TLS <sup>1</sup> | PEAP-TLS <sup>2</sup> | PEAP EAP-MSCHAPv2 | EAP-FAS T MSCHAP v2 | PEAP-GTC | EAP-FAS T-GTC |
|-----------------------|---------|----------------------|-----------------------|-------------------|---------------------|----------|---------------|
| ACS                   | Yes     | Yes <sup>3</sup>     | Yes                   | Yes               | Yes                 | Yes      | Yes           |
| Windows AD            | No      | Yes                  | Yes                   | Yes               | Yes                 | Yes      | Yes           |
| LDAP                  | No      | Yes                  | Yes                   | No                | No                  | Yes      | Yes           |
| RSA Identity Store    | No      | No                   | No                    | No                | No                  | Yes      | Yes           |
| RADIUS Identity Store | No      | No                   | No                    | No                | No                  | Yes      | Yes           |

1. In EAP-TLS authentication, the user is authenticated by cryptographic validation of the certificate. Additionally, ACS 5.8.1 optionally allows a binary comparison of the user's certificate sent by the end-user client against the certificate located in the user's record in the LDAP identity store.
2. In PEAP-TLS authentication, the user is authenticated by cryptographic validation of the certificate. Additionally, ACS 5.8.1 optionally allows a binary comparison of the user's certificate sent by the end-user client against the certificate located in the user's record in the LDAP identity store.
3. ACS Identity Store cannot store the certificates.



## Open Source License Acknowledgments

---

See [http://www.cisco.com/en/US/products/ps9911/products\\_licensing\\_information\\_listing.html](http://www.cisco.com/en/US/products/ps9911/products_licensing_information_listing.html) for all the Open Source and Third Party Licenses used in Cisco Secure Access Control System, 5.8.1.

### Notices

The following notices pertain to this software license.

### OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

### License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).

#### OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)".

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact [openssl-core@openssl.org](mailto:openssl-core@openssl.org).
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:  
“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). This product includes software written by Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

**Original SSLeay License:**

Copyright © 1995-1998 Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)). All rights reserved.

This package is an SSL implementation written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com)).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson ([tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young ([ey@cryptsoft.com](mailto:ey@cryptsoft.com))”.

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptography-related.



4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”.

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

